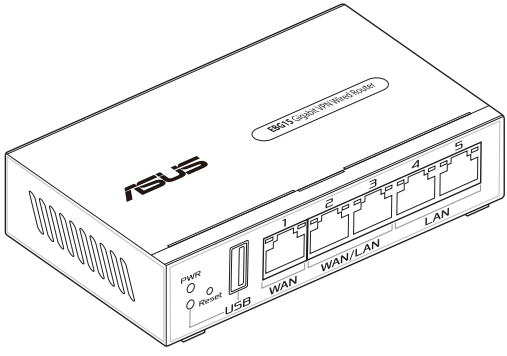
User Guide

ASUS EBG15

Gigabit VPN Wired Router

Model: EBG15



IN SEARCH OF INCREDIBLE

E23348
First Edition
April 2024

Copyright © 2024 ASUSTeK Computer Inc. All Rights Reserved.

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK Computer Inc. ("ASUS").

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification of alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

ASUS PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ASUS, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS AND THE LIKE), EVEN IF ASUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS MANUAL OR PRODUCT.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ASUS. ASUS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

Table of contents

1 Getting to know your EBG15

1.1 Welcome! 7
1.2 Package contents 7
1.3 Your wired router 8
1.4 Positioning your router 10
1.5 Setup Requirements 11
1.6 Router Setup 12
1.6.1 Wired connection 13

2 Getting started

2.1 Logging into the Web GUI 14
2.2 Auto-detection of WAN 15

3 Configuring EBG15

3.1 Adaptive QoS 17
3.1.1 Bandwidth Monitor 17
3.1.2 QoS 18
3.1.3 Web History 18
3.1.4 Internet Speed 19
3.2 Administration 20
3.2.1 Operation Mode 20
3.2.2 System 21
3.2.3 Firmware Upgrade 22
3.2.4 Restore/Save/Upload Setting 23
3.2.5 Feedback 24
3.2.6 Privacy 25
3.3 AiMesh 26
3.3.1 Setting up the ExpertWiFi AiMesh system 26
3.3.2 Managing your network clients 27
3.4 AiProtection 28
3.4.1 Network Protection 28

Table of contents

3.5 Dashboard 32

3.6 Device access control 33

3.6.1 Web & Apps Filters 33

3.6.2 Time Scheduling 34

3.7 Firewall 35

3.7.1 General 35

3.7.2 URL Filter 36

3.7.3 Keyword filter 37

3.7.4 Network Services Filter 38

3.8 IPv6 39

3.9 LAN 40

3.9.1 LAN IP 40

3.9.2 DHCP Server 41

3.9.3 Route 43

3.9.4 IPTV 44

3.9.5 Switch Control 44

3.9.6 VLAN 45

3.10 Network Tools 47

3.10.1 Network Analysis 47

3.10.2 Netstat 47

3.10.3 Wake on LAN 47

3.10.4 Smart Connect Rule 47

3.11 Self-Defined Network 48

3.11.1 Employee 49

3.11.2 Guest Portal 49

3.11.3 Guest Network 50

3.11.4 Scheduled Network 50

3.11.5 IoT Network 51

3.11.6 VPN Network 51

3.11.7 Scenario Explorer 52

Table of contents

3.11.8 Customized Network 53
3.12 System Log 54
3.13 Traffic Analyzer 55
3.13.1 Traffic Analyzer 55
3.14 USB Application 56
3.14.1 Media Server 56
3.14.2 Network Place (Samba) Share 57
3.14.3 FTP Share 57
3.14.4 Network Printer Server 58
3.14.5 USB Modem 66
3.15 VPN Fusion 67
3.15.1 Creating a VPN fusion 67
3.15.2 Internet Connection 68
3.16 VPN Server 69
3.16.1 PPTP 69
3.16.2 OpenVPN 70
3.16.3 IPSec VPN 71
3.16.4 WireGuard® VPN 72
3.17 WAN 73
3.17.1 Internet Connection 73
3.17.2 Multi-WAN 75
3.17.3 Port Trigger 77
3.17.4 Virtual Server/Port Forwarding 79
3.17.5 DMZ 82
3.17.6 DDNS 83
3.17.7 NAT Passthrough 84
3.18 Wireless 85
3.18.1 General 85
3.18.2 Wireless MAC Filter 86

3.18.3 Roaming Block List 87

4 Troubleshooting

4.1 Basic Troubleshooting 88

4.2 Frequently Asked Questions (FAQs) 90

Appendices

Safety Notices 107

Service and Support 109

1 Getting to know your EBG15

1.1 Welcome!

Thank you for purchasing an ASUS EBG15!

EBG15 provides a fast, secure and scalable network, enhanced network stability through Ethernet connectivity and provides internet backup with two WAN/LAN ports and one USB port to support the operations.

1.2 Package contents

- ☑ EBG15
- ☑ Power adapter
- ☑ Quick Start Guide
- ☑ Network cable (RJ-45)
- ☑ Local login information sticker
- ☑ Warranty card

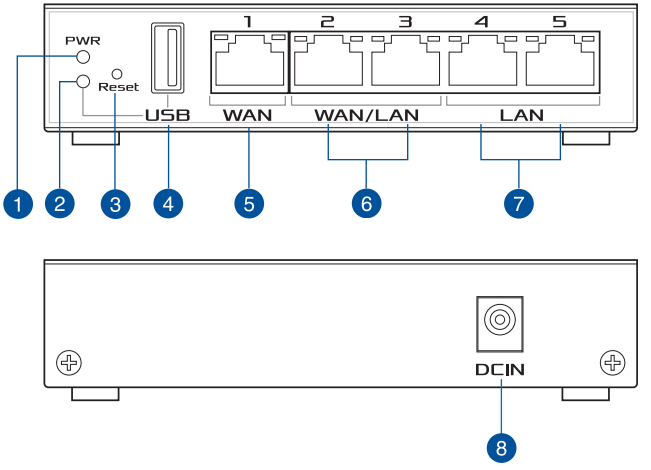
NOTES:

- If any of the items are damaged or missing, contact ASUS for technical inquiries and support. Refer to **Service and Support** at the back of this user manual.
- Keep the original packaging material in case you would need future warranty services such as repair or replacement.

1.3 Your wired router

1. Plug the adapter into the DCIN port.
2. The power LED will light up when your hardware is ready.

Button and Port Explanations



1	**Power LED** **Off**: No power. **On**: Device is ready. **Flashing slow**: Rescue mode.
2	**USB 3.2 Gen 1 LED** **Off**: No power or no physical connection. **On**: Device is ready. **Flashing slow**: Transmitting or receiving data.
3	**Reset button** This button resets or restores the system to its factory default settings.
4	**USB 3.2 Gen 1 port** Insert a USB 3.2 Gen 1 device such as a USB hard disk or a USB flash drive into this port.
5	**WAN (Internet) port** Connect a network cable into this port to establish WAN connection.
6	**WAN / LAN ports** Connect a network cable into this port to establish WAN / LAN connection.
7	**LAN ports** Connect your PC to a LAN port with a network cable.
8	**Power (DCIN) port** Insert the bundled AC adapter into this port and connect your router to a power source.

Ethernet port LED indications

LED Indicators			
Speed LED (Green)		Link/Act LED (Amber)	
1G	ON	1G/100M/10M	Blinking
100M/10M	OFF	No Traffic	ON

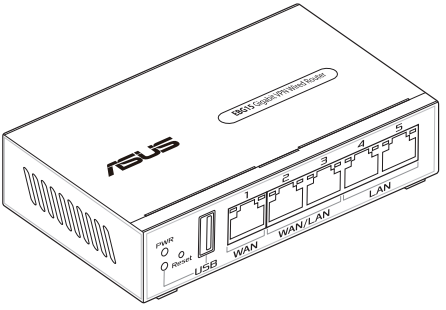
Specifications:

DC Power adapter	DC Output: +12V with max 1.5A current		
Operating Temperature	0~40°C	Storage	0~70°C
Operating Humidity	50~90%	Storage	20~90%

1.4 Positioning your router

For the best networking experience, ensure that you:

- Always update to the latest firmware. Visit the ASUS website at **http://www.asus.com** to get the latest firmware updates.



1.5 Setup Requirements

To set up your network, you need a computer that meets the following system requirements:

- Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/ 1000BaseTX)
- An installed TCP/IP service
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

NOTE: The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

1.6 Router Setup

IMPORTANT!

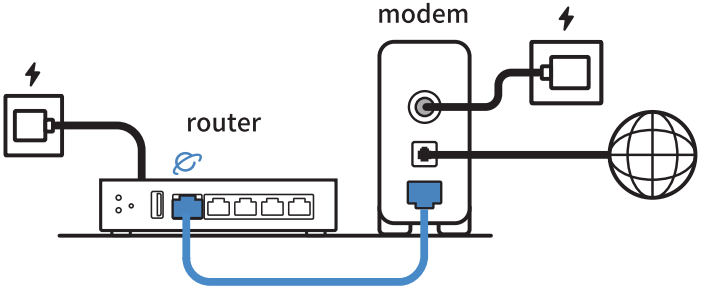
- Before setting up your ASUS wired router, do the following:
  - If you are replacing an existing router, disconnect it from your network.
  - Disconnect the cables/wires from your existing modem setup. If your modem has a backup battery, remove it as well.
  - Reboot your cable modem and computer (recommended).

WARNING!

- The power supply cord(s) must be plugged into socket-outlet(s) that is /are provided with a suitable earth ground. Connect the equipment only to a nearby socket outlet that is easily accessible.
- If the adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- DO NOT use damaged power cords, accessories, or other peripherals.
- DO NOT mount this equipment higher than 2 meters.
- Use this product in environments with ambient temperatures between 0°C (32°F) and 40°C (104°F).

1.6.1 Wired connection

NOTE: You can use either a straight-through cable or a crossover cable for wired connection.



To set up your wired router via wired connection:

1. Insert your wired router's AC adapter to the DCIN port and plug it to a power outlet.
2. Using the bundled network cable, connect your computer to your wired router's LAN port.
3 Using another network cable, connect your modem to your wired router's WAN port.
4. Insert your modem's AC adapter to the DCIN port and plug it to a power outlet.

2 Getting started

2.1 Logging into the Web GUI

Your ASUS Wired Router comes with an intuitive web graphical user interface (GUI) that allows you to easily configure its various features through a web browser such as Microsoft Edge, Safari, or Google Chrome.

NOTE: The features may vary with different firmware versions.

Connecting to your network wiredly:

To log into the web GUI:

1. On your web browser, enter http://expertwifi.net.
2. Follow the instructions for setup.

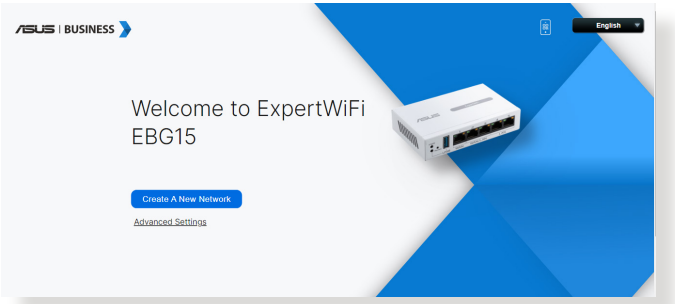
2.2 Auto-detection of WAN

The Quick Internet Setup (QIS) function guides you in quickly setting up your Internet connection.

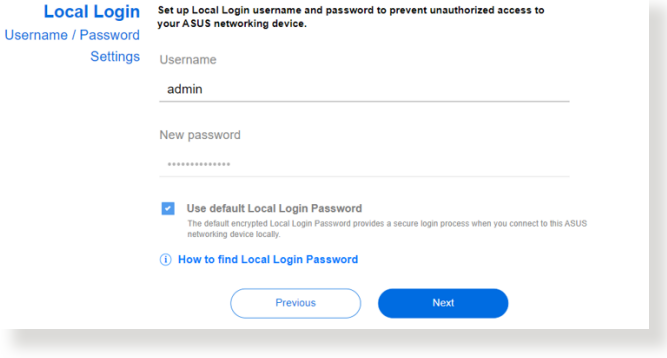
NOTE: When setting the Internet connection for the first time, press the Reset button on your wired router to reset it to its factory default settings.

Auto-detection of WAN:

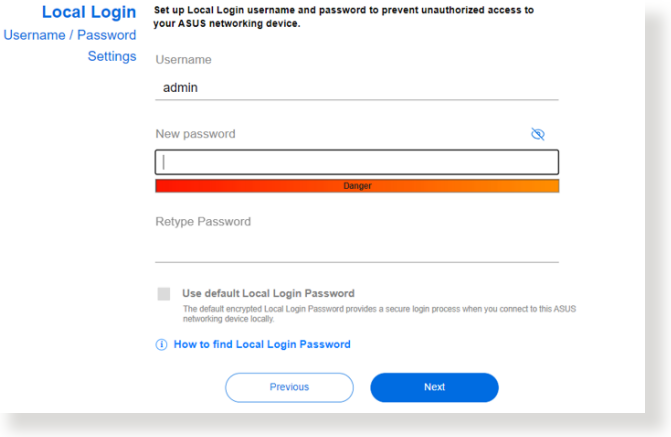
1. Log into the Web GUI and click **Create A New Network**.



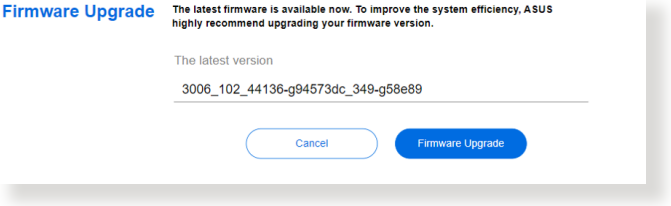
2. Click **Next** to log in with the default username and password.



Untick **Use default Local Login Password**, and enter a new username and password, then click **Next**.



3. Click **Firmware Upgrade** to upgrade the firmware to the latest or click **Cancel** to keep the current version.



NOTE: The screen appears only when a new firmware version is available.

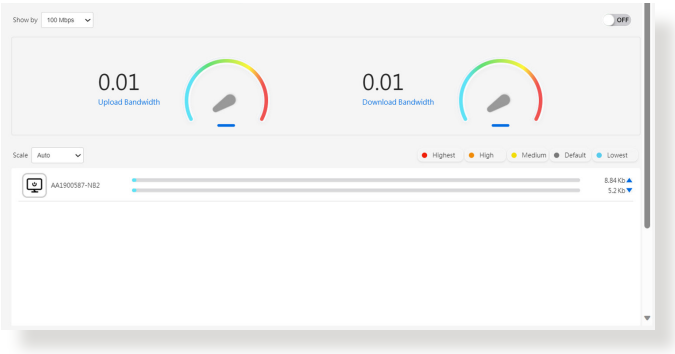
3 Configuring EBG15

3.1 Adaptive QoS

3.1.1 Bandwidth Monitor

Bandwidth Monitor allows you to monitor the total and each client's download and upload bandwidth usage.

To use **Bandwidth Monitor**, go to **Settings** > **Adaptive QoS** > **Bandwidth Monitor**.

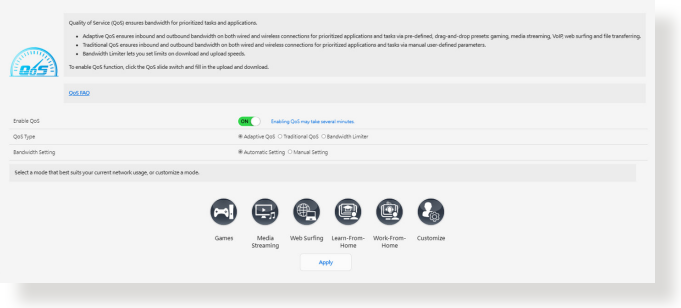


NOTE: For more information, please visit https://www.asus.com/support/faq/1008717.

3.1.2 QoS

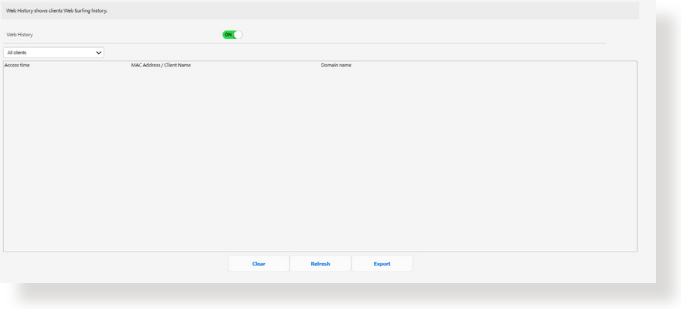
Quality of Service (QoS) ensures the bandwidth for prioritized tasks and applications.

1. **Adaptive QoS** ensures inbound and outbound bandwidth on both wired and wireless connections for prioritized applications and tasks via pre-defined, drag-and-drop presets: gaming, media streaming, VoIP, web browsing and file transfer.
2. **Traditional QoS** ensures inbound and outbound bandwidth on both wired and wireless connections for prioritized applications and tasks via manual user-defined parameters.
3. **Bandwidth Limiter** lets you set limits on download and upload speeds.



3.1.3 Web History

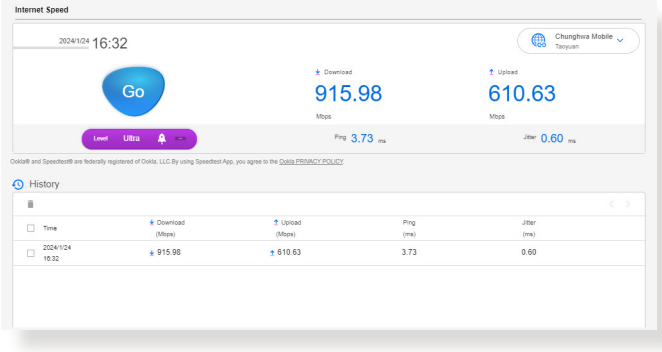
Web History page displays the clients' web browsing history.



3.1.4 Internet Speed

This service is provided by Ookla®. It detects the download and upload speed from your router to the Internet.

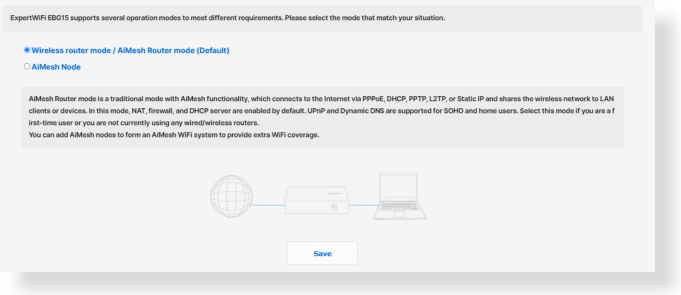
Click **GO** to have an internet speed test, which takes approximately one minute to complete.



3.2 Administration

3.2.1 Operation Mode

The Operation Mode page allows you to select the appropriate mode for your network.



To set up the operating mode:

1. From the navigation panel, go to **Settings** > **Administration** > **Operation Mode**.
2. Select any of these operation modes:
   - **Wireless router mode / AiMesh Router mode (Default):** AiMesh Router mode is a traditional mode with AiMesh functionality, which connects to the Internet via PPPoE, DHCP, PPTP, L2TP, or Static IP and shares the wireless network to LAN clients or devices. In this mode, NAT, firewall, and DHCP server are enabled by default. UPnP and Dynamic DNS are supported for SOHO and home users.
   - **AiMesh Node**: You can add AiMesh nodes to form an AiMesh WiFi system to provide extra WiFi coverage.
3. Click **Save**.

NOTE: The router will reboot when you change the modes.

3.2.2 System

The **System** page allows you to configure your wired router settings.

To set up the System settings:

1. From the navigation panel, go to **Settings** > **Administration** > **System**.
2. You can configure the following settings:
   - **Change router login password**: You can change the password and login name for the wired router by entering a new name and password.
   - **USB setting**: You can Enable HDD Hibernation and change USB mode.
   - **Time Zone**: Select the time zone for your network.
   - **NTP Server**: The wired router can access a NTP (Network time Protocol) server in order to synchronize the time.
   - **Network Monitoring**: You can enable DNS Query to check Resolve Hostname and Resolved IP Addresses, or enable Ping, then check your Ping Target.
   - **Auto Logout**: You can set the time of auto-logout.
   - **Enable WAN down browser redirect notice:** This feature allows the browser to display a warning page when the router is disconnected from Internet. When disabled, the warning page will not appear.
   - **Enable Telnet**: Click **Yes** to enable Telnet services on the network. Click **No** to disable Telnet.
   - **Authentication Method**: You can select HTTP, HTTPS, or both protocols to secure router access.
   - **Enable Reboot Scheduler:** When enabled, you can set the Date to Reboot and Time of Day to Reboot.
   - **Enable Web Access from WAN**: Select **Yes** to allow devices outside the network to access the wired router GUI settings. Select **No** to prevent access.
   - **Enable Access Restrictions**: Click **Yes** if you want to specify the IP addresses of devices that are allowed to access to the wired router GUI settings from WAN/LAN.

- **Service**: This feature allows you to configure Enable Telnet/ Enable SSH/SSH Port/Allow Password Login/Authorized Keys/Idle Timeout.

3. Click **Apply**.

3.2.3 Firmware Upgrade

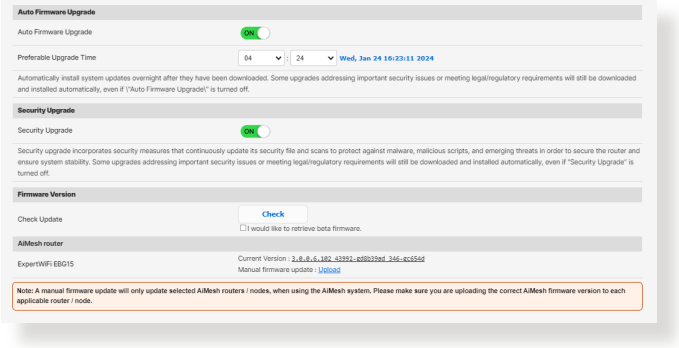
NOTE: Download the latest firmware from the ASUS website at **http://www.asus.com**.

To upgrade the firmware:

1. From the navigation panel, go to **Settings** > **Administration** > **Firmware Upgrade**.
2. In the **New Firmware File** field, click **Browse** to locate the downloaded file.
3. Click **Upload**.

NOTES:

- When the upgrade process is complete, wait for some time for the system to reboot.
- If the upgrade process fails, the wired router automatically enters rescue mode and the power LED indicator on the front panel starts flashing slowly.

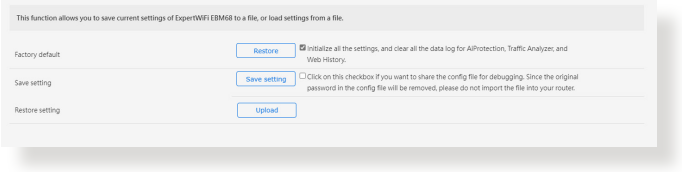


3.2.4 Restore/Save/Upload Setting

To restore/save/upload wired router settings:

1. From the navigation panel, go to **Settings** > **Administration** > **Restore/Save/Upload Setting**.
2. Select the tasks that you want to do:
   - **Factory default**: Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer and Web History.
   - **Save setting**: Click on this checkbox if you want to share the configuration file for debugging. Since the original password in the configuration file will be removed, please do not import the file into your router.
   - **Restore setting**: Upload the restoration settings you want to apply.

IMPORTANT! If issues occur, upload the latest firmware version and configure new settings. Do not restore the router to its default settings.



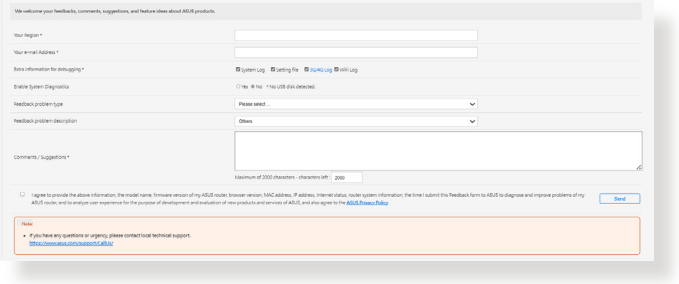
3.2.5 Feedback

To use Feedback:

1. From the navigation panel, go to **Settings** > **Administration** > **Feedback**.
2. Enter your region, e-mail address, extra information for debugging, comments and suggestions, and send your router log back for troubleshooting.

IMPORTANT!

- Describe your comments on the situation in details to get a quick response.
- Please agree with the ASUS Privacy Policy.



3.2.6 Privacy

1. For account binding, DDNS and Remote connection (ASUS Router app/Lyra app/AiCloud/AiDisk):

Please note that your information, including your product model name, firmware version, Internet status, IP Address, MAC address and DDNS name, will be collected by ASUS through the above functions.

If you want to disable sharing your information with ASUS through the above functions, please click **Withdraw** below. However, please note that these features/functions may not work if you stop sharing your information with ASUS.

IMPORTANT!

- After you click **Withdraw**, there will be some changes as listed below:
  - The DDNS name you are currently using will not be kept in your router.
  - ASUS Router app, Lyra app, AiCloud, AiDisk can be used only when your device is in the same LAN with the router.

---

2. ASUS PRIVACY Notice (for firmware/security upgrade):

Please note that your information will be collected by ASUS router for firmware/security upgrade purposes. If you want to disable sharing your information with ASUS router, please click **Withdraw** below.

IMPORTANT! Clicking **Withdraw** here may result in the failure of upgrading to the latest firmware and getting the most up-to-date protection on your ASUS router. However, to protect the security of your router and ensure the compliance with laws, upgrades addressing important security issues or meeting legal/regulatory requirements will still be downloaded and installed automatically.

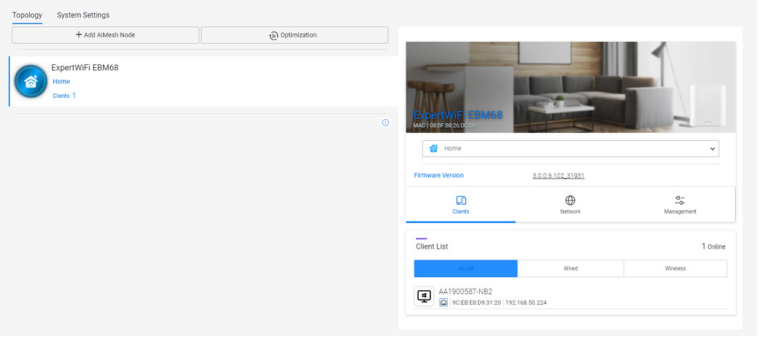
3.3 AiMesh

3.3.1 Setting up the ExpertWiFi AiMesh system

To build up your ExpertWiFi AiMesh system, you need to configure its settings.

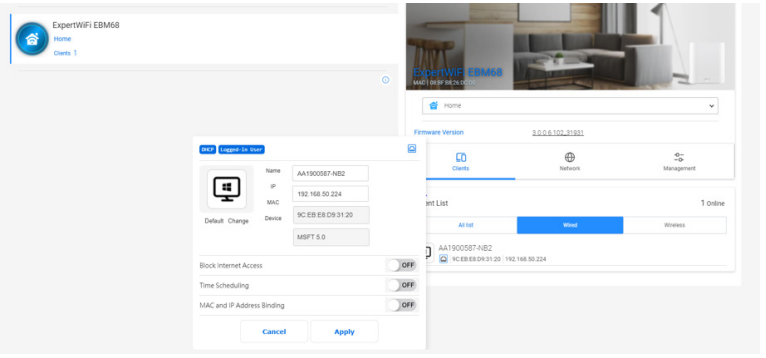
To set up the ExpertWiFi AiMesh system settings:

1. From the navigation panel, go to **AiMesh** > **Topology**.
2. You can click the bottom of **Set up as AiMesh Node** to add the ExpertWiFi devices under the control of EBG15.



3. Go to **AiMesh** > **System Settings** to enable or disable **AiMesh node Ethernet auto setup**, **Ethernet Backhaul Mode,** configure **Roaming Block List**, **System Reset to Factory Default** or **System Reset**.

3.3.2 Managing your network clients

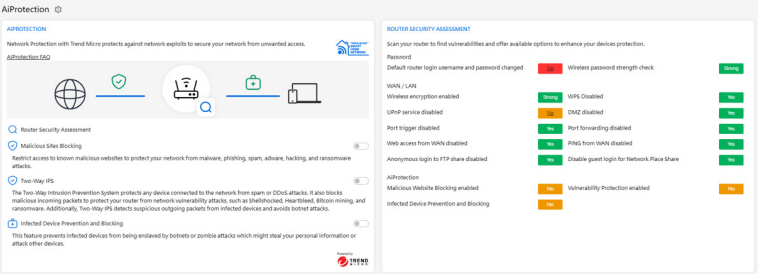


To manage your network clients:

1. From the navigation panel, go to **AiMesh** > **Topology**.
2. Select the **Clients** icon to display your network client's information such as the client's name, MAC and IP address.
3. You can block the client's access to your network, disable its time scheduling or disable its MAC and IP binding by moving the slider to **OFF**.
4. Click **Apply** when done.

3.4 AiProtection

AiProtection provides real-time monitoring that detects malware, spyware, and unwanted access. It also filters unwanted websites and apps and allows you to schedule a time that a connected device is able to access the Internet.

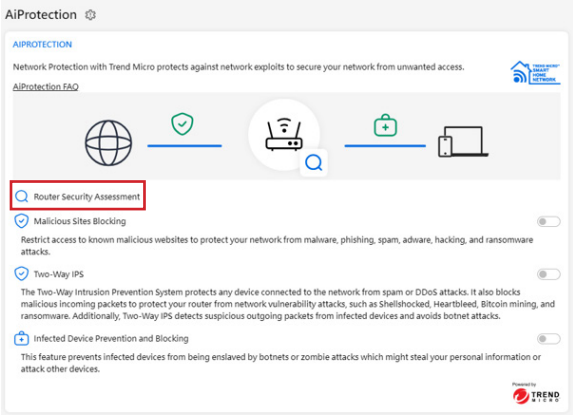


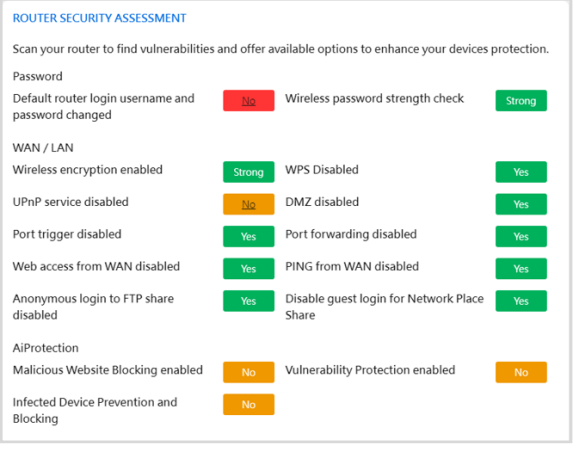
3.4.1 Network Protection

Network Protection prevents network exploits and secures your network from unwanted access.

To assess your router security:

1. From the navigation panel, go to **AiProtection**.
2. Click **Router Security Assessment** to display the security assessment results.





IMPORTANT! Items marked as **Yes** on the **ROUTER SECURITY ASSESSMENT** page are considered to be at a safe status. Items marked as **No** are highly recommended to be configured accordingly.

3. (Optional) From the **ROUTER SECURITY ASSESSMENT** page, manually configure the items marked as **No**. To do this:

   a. Click an item.

NOTE: When you click an item, the utility forwards you to the item's setting page.

b. From the item's security settings page, configure and make the necessary changes and click **Apply** when done.

c. Go back to the **ROUTER SECURITY ASSESSMENT** page and click **Close** to exit the page.

4. To automatically configure the security settings, click **Secure Your Router.**
5. When a message prompt appears, click **OK**.

To enable the network protection:

1. From the navigation panel, go to **AiProtection**.
2. Select the type of protection you want to implement and slide it on. You can choose among **Malicious Sites Blocking**, **Two-Way IPS** and **Infected Device Prevention and Blocking**.

Malicious Sites Blocking

This feature restricts access to known malicious websites to protect your network from malware, phishing, spam, adware, hacking and ransomware attacks.

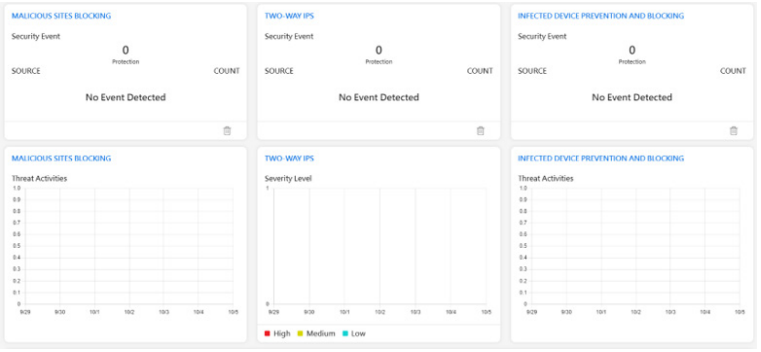
Two-Way IPS

Two-Way IPS (Intrusion Prevention System) protects the connected devices from spam or DDoS attacks. It also blocks malicious incoming packets to protect your router from network vulnerability attacks, such as Shellshocked, Heartbleed, Bitcoin mining, and ransomware. Additionally, Two-Way IPS detects suspicious outgoing packets from infected devices and avoids botnet attacks.

Infected Device Prevention and Blocking

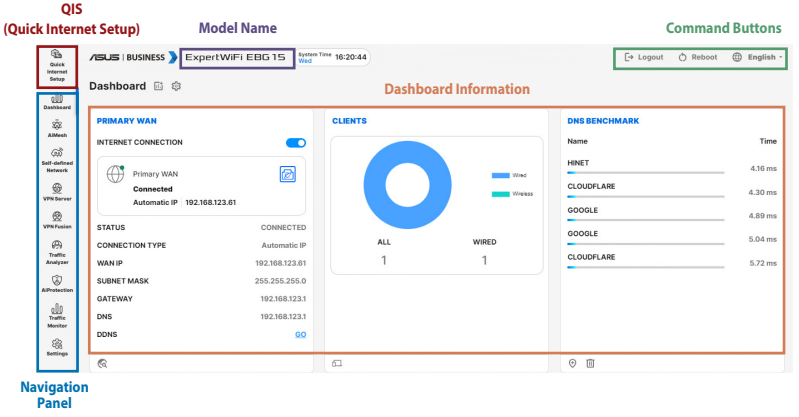
This feature prevents infected devices from being enslaved by botnets or zombie attacks which might steal your personal information or attack other devices.

3. Agree with **Trend Micro End User License Agreement**.


MALICIOUS SITES BLOCKING
Security Event
0
Protection
SOURCE
COUNT
No Event Detected
TWO-WAY IPS
Security Event
0
Protection
SOURCE
COUNT
No Event Detected
INFECTED DEVICE PREVENTION AND BLOCKING
Security Event
0
Protection
SOURCE
COUNT
No Event Detected
MALICIOUS SITES BLOCKING
Threat Activities
TWO-WAY IPS
Severity Level
High
Medium
Low
INFECTED DEVICE PREVENTION AND BLOCKING
Threat Activities

3.5 Dashboard

Dashboard allows you to manage your network such as internet connection, client connection, DNS benchmark, system status, ethernet port, and traffic monitor.



3.6 Device access control

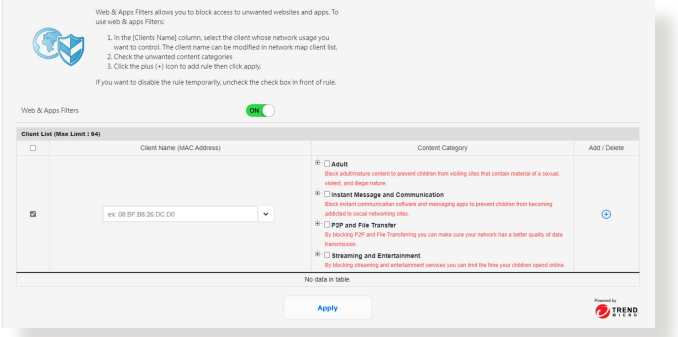
3.6.1 Web & Apps Filters

Web & Apps Filters allows you to block access to unwanted websites and apps.

To use Web & Apps Filters:

1. From the navigation panel, go to **Settings** > **Device access control** > **Web & Apps Filters**.
2. Slide the bar to **ON** to enable **Web & Apps Filters**.
3. In the **Client Name** column, select the client on which you want to control the network usage. The client name can be modified in the network map client list.
4. Check the unwanted content categories.
5. Click ⊕ to add a rule and click **Apply**.

If you want to disable a rule temporarily, uncheck the rule.

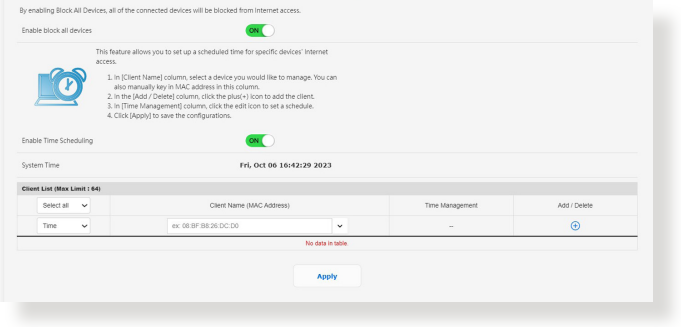


3.6.2 Time Scheduling

Time Scheduling allows you to set up a scheduled time for specific devices' Internet access.

To use Time Scheduling:

1. From the navigation panel, go to **Settings** > **Device access control** > **Time Scheduling**.
2. Slide the bar to **ON** to enable **Enable Time Scheduling**.
3. From the **Client Name** column, select or key in the client's name from the drop down list box.
4. Click ⊕ to add the client's profile.
5. Click **Apply** to save the settings.



3.7 Firewall

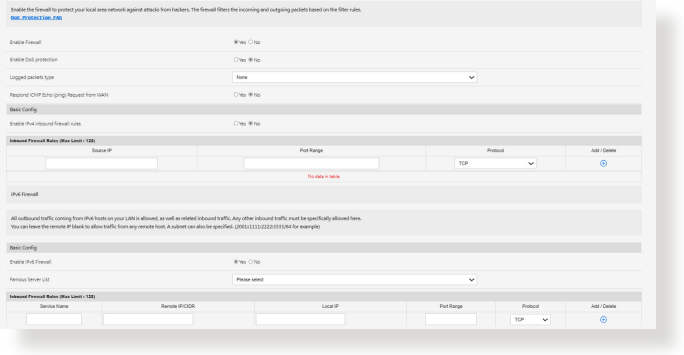
3.7.1 General

The wired router can serve as a hardware firewall for your network.

NOTE: The Firewall feature is enabled by default.

To set up basic Firewall settings:

1. From the navigation panel, go to **Settings** > **Firewall** > **General**.
2. On the **Enable Firewall** field, select **Yes**.
3. On the **Enable DoS** protection, select **Yes** to protect your network from DoS (Denial of Service) attacks though this may affect your router's performance.
4. You can also monitor packets exchanged between the LAN and WAN connection. On the Logged packets type, select **Dropped**, **Accepted**, or **Both**.
5. Click **Apply**.



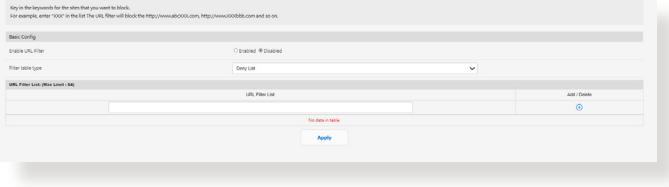
3.7.2 URL Filter

You can specify keywords or web addresses to prevent access to specific URLs.

NOTE: The URL Filter is based on a DNS query. If a network client has already accessed a website such as http://www.abcxxx.com, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the URL Filter.

To set up a URL filter:

1. From the navigation panel, go to **Settings** > **Firewall** > **URL Filter**.
2. On the **Enable URL Filter** field, select **Enabled**.
3. Enter a URL and click ⊕.
4. Click **Apply**.



3.7.3 Keyword filter

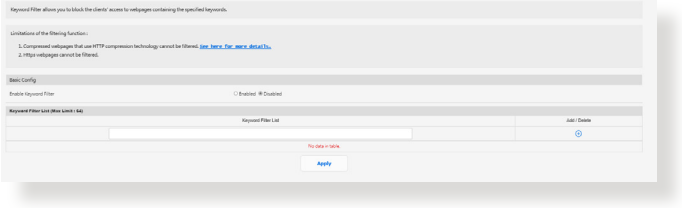
Keyword filter blocks access to webpages containing specified keywords.

To set up a keyword filter:

1. From the navigation panel, go to **Settings** > **Firewall** > **Keyword Filter**.
2. On the **Enable Keyword Filter** field, select **Enabled**.
3. Enter a word or phrase and click ⊕.
4. Click **Apply**.

NOTES:

- The Keyword Filter is based on a DNS query. If a network client has already accessed a website such as http://www.abcxxx.com, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the Keyword Filter.
- Web pages compressed using HTTP compression cannot be filtered. HTTPS pages also cannot be blocked using a keyword filter.

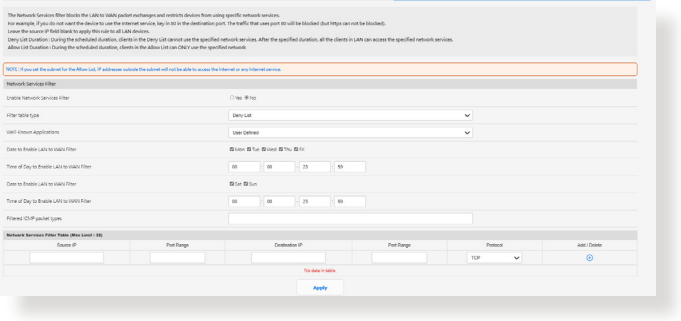


3.7.4 Network Services Filter

The Network Services Filter blocks LAN to WAN packet exchanges and restricts network clients from accessing specific web services such as Telnet or FTP.

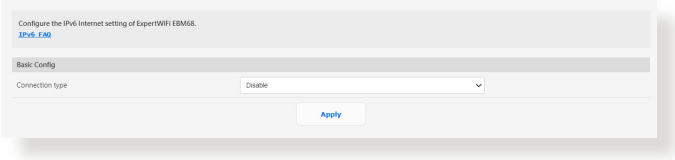
To set up a Network Service filter:

1. From the navigation panel, go to **Settings** > **Firewall** > **Network Service Filter**.
2. On the **Enable Network Services Filter** field, select **Yes**.
3. Select the Filter table type. **Deny List** blocks the specified network services. **Allow List** limits access to only the specified network services.
4. Specify the day and time when the filters will be active.
5. To specify a Network Service to filter, enter the Source IP, Destination IP, Port Range, and Protocol. Click ⊕.
6. Click **Apply**.



3.8 IPv6

This wired router supports IPv6 addressing, a system that supports more IP addresses. Contact your ISP if your Internet service supports IPv6.



To set up IPv6:

1. From the navigation panel, go to **Settings** > **IPv6**.
2. Select your **Connection type**. The configuration options vary depending on your selected connection type.
3. Enter your IPv6 LAN and DNS settings.
4. Click **Apply**.

NOTES:

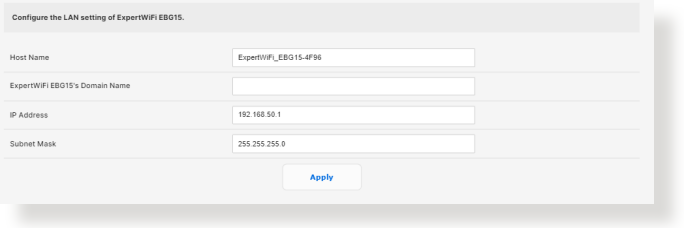
- Please refer to your ISP regarding specific IPv6 information for your Internet service.
- For more information, please visit https://www.asus.com/support/FAQ/113990.

3.9 LAN

3.9.1 LAN IP

The LAN IP screen allows you to modify the LAN IP settings of your wired router.

NOTE: Any changes to the LAN IP address will be reflected on your DHCP settings.

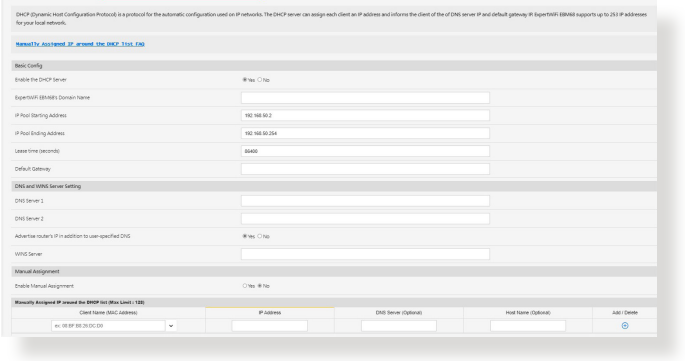


To modify the LAN IP settings:

1. From the navigation panel, go to **Settings** > **LAN** > **LAN IP**.
2. Modify the **IP Address** and **Subnet Mask**.
3. When done, click **Apply**.

3.9.2 DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign an IP address to each client and inform the client of the DNS server IP and default gateway IP.



To configure the DHCP server:

1. From the navigation panel, go to **Settings** > **LAN** > **DHCP Server**.
2. In the **Enable the DHCP Server** field, tick **Yes**.
3. In the **Domain Name** text box, enter a domain name for the wired router.
4. In the **IP Pool Starting Address** field, key in the starting IP address.
5. In the **IP Pool Ending Address** field, key in the ending IP address.
6. In the **Lease Time** field, specify in seconds when an assigned IP address will expire. Once it reaches this time limit, the DHCP server will then assign a new IP address.

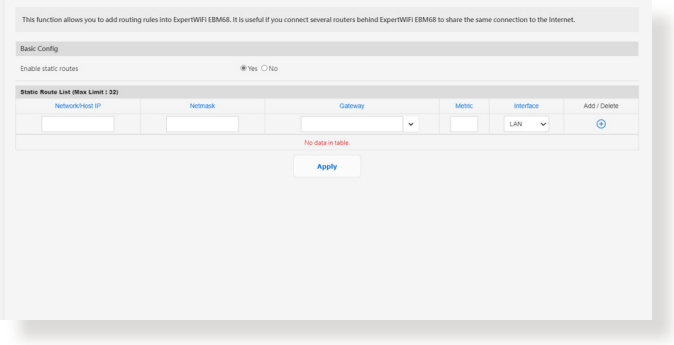
NOTES:

- We recommend that you use an IP address format of 192.168.1.xxx (where xxx can be any number between 2 and 254) when specifying an IP address range.
- An IP Pool Starting Address should not be greater than the IP Pool Ending Address.

7. In the **DNS and Server Settings** section, key in your DNS Server and WINS Server IP address if needed.
8. Your wired router can also manually assign IP addresses to devices on the network. On the **Enable Manual Assignment** field, choose **Yes** to assign an IP address to specific MAC addresses on the network. Up to 32 MAC Addresses can be added to the DHCP list for manual assignment.

3.9.3 Route

This function allows you to add routing rules to the router. It is useful if you connect several routers behind EBG15 to share the same connection to the Internet.

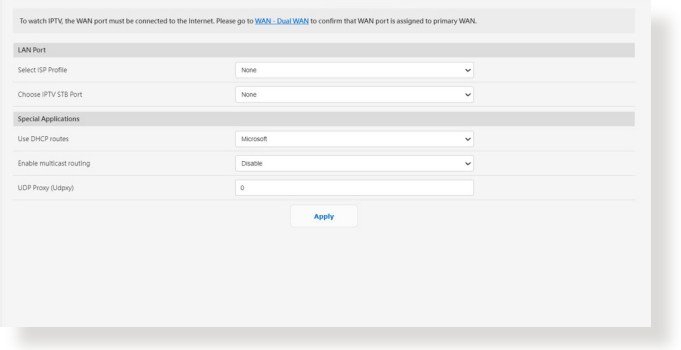


To configure the LAN Routing table:

1. From the navigation panel, go to **Settings** > **LAN** > **Route**.
2. On the **Enable static routes** field, choose **Yes**.
3. On the **Static Route List**, enter the network information of other access points or nodes. Click ⊕ or ⊖ to add or remove a device on the list.
4. Click **Apply**.

3.9.4 IPTV

The wired router supports connection to IPTV services through an ISP or a LAN. The IPTV tab provides the configuration settings needed to set up IPTV, VoIP, multicasting, and UDP for your service. Contact your ISP for specific information regarding your service.

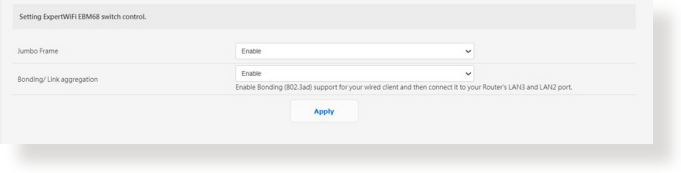


3.9.5 Switch Control

Allows you to set up the router for the function of switch control. You can combine two 1Gbps LAN ports to deliver up to 2Gbps wired speeds via bonding to your compatible NAS or other high-bandwidth network device.

NOTES:

- To use the Link Aggregation Control Protocol (LACP) function, the devices must support IEEE 802.3ad protocol.
- The LAN aggregation function can be operated by pairing the LAN3 port with the LAN2 port.

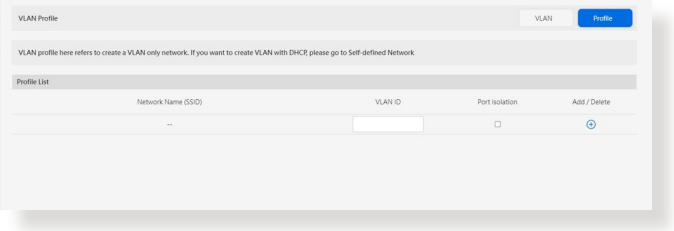


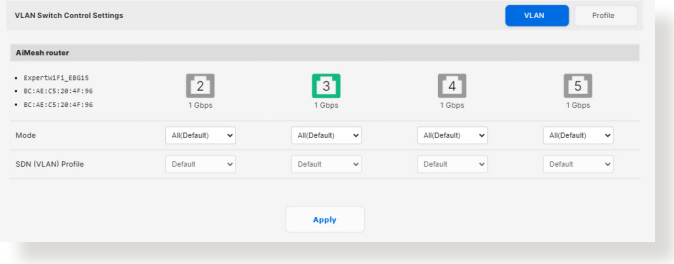
3.9.6 VLAN

A VLAN (Virtual Local Area Network) is a logical network created within a larger physical network. VLANs allow you to segment a network into smaller, virtual sub-networks, which can be used to isolate traffic and improve network performance.

To set up VLAN:

1. From the navigation panel, go to **Settings** > **LAN** > **VLAN**.
2. Click the **Profile** tab and then ⊕ to create a VLAN profile. You can assign your own VLAN ID.
3. **Port isolation** restricts the access right of different devices in the same VLAN. You are now creating a "VLAN-only-Network", which means a network with VID but without DHCP.





4. Click **VLAN** tab to select a port with specific profile and mode (**Trunk** / **Access**).

NOTE: You can select one of the following default modes:

All (Default) allows all tagged and untagged packets to access.

Access mode allows a selected SDN(VLAN) to access. You can select profiles created by Guest Network pro or by VLAN.

Trunk mode:

- **Allow all tagged:** Only tagged packets are allowed to access.
- **With selected SDN(VLAN):** Only selected SDN or VLAN is allowed to access.

5. When done, click **Apply**.

NOTE: For more information, please visit https://www.asus.com/support/FAQ/1049415/.

3.10 Network Tools

To use network tools, from the navigation panel, go to **Settings** > **Network Tools**.

3.10.1 Network Analysis

Send ICMP ECHO_REQUEST packets to network hosts.

3.10.2 Netstat

Display the network details.

3.10.3 Wake on LAN

The WOL (Wake-On-LAN) feature lets you wake up a computer from any device in the network.

3.10.4 Smart Connect Rule

Set up the Smart Connect related information.

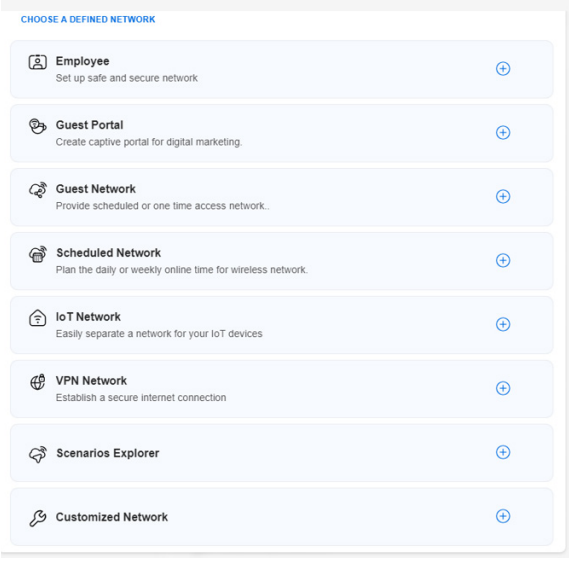
3.11 Self-Defined Network

A Self-Defined Network (SDN) provides up to five SSIDs to separate and prioritize devices for different business uses and network alternatives, creating network segments for employees, guest portals, guest networks, scheduled networks, IoT networks and VPN networks.

IMPORTANT! To make the Wi-Fi function available, ensure to integrate a wireless Access Point (AP) such as ExpertWiFi EBA63 or router such as ExpertWiFi EBR63 or ExpertWiFi EBM68 into the EBG15's AiMesh network.

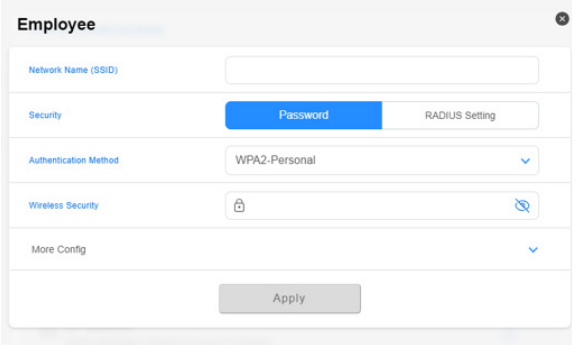
To create a Self-Defined Network:

1. From the navigation panel, go to **Self-Defined Network**.
2. Choose a defined network that fits your specific scenario.



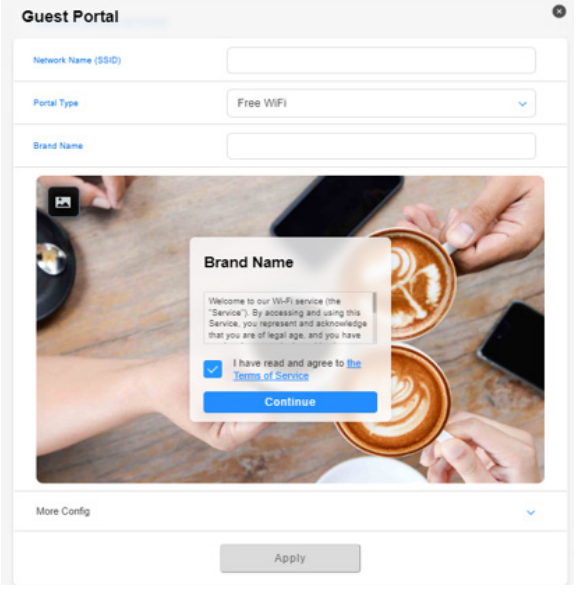
3.11.1 Employee

Allows you to set up access level for different uses to enhance network security. Recommended for offices that assign permissions to different departments.



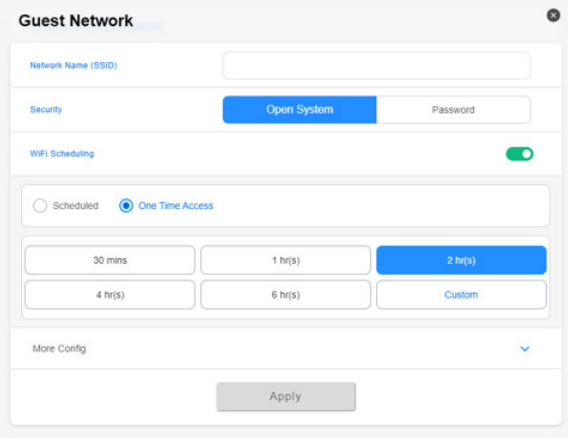
3.11.2 Guest Portal

Enables you to create a guest portal for digital marketing. Recommended for use in restaurants, hotels or food trucks.



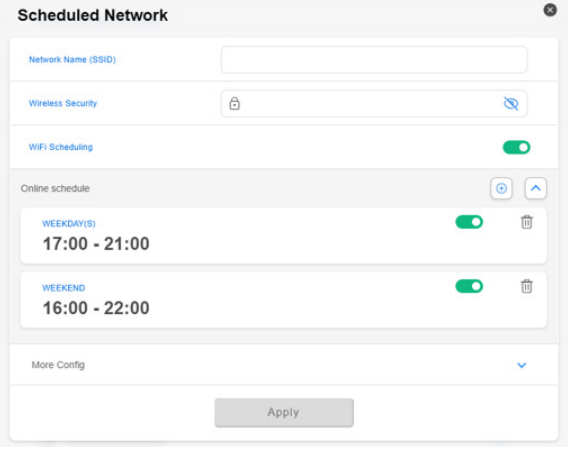
3.11.3 Guest Network

Provides temporary visitors with scheduled or one time access to the network. Recommended for use in shopping malls, gyms or for visitors.



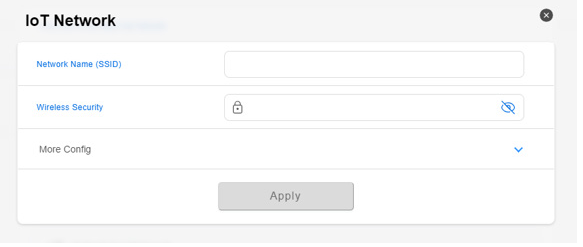
3.11.4 Scheduled Network

Plans the daily or weekly online time for the wireless network. Recommended for distance learning, classroom or children's use.



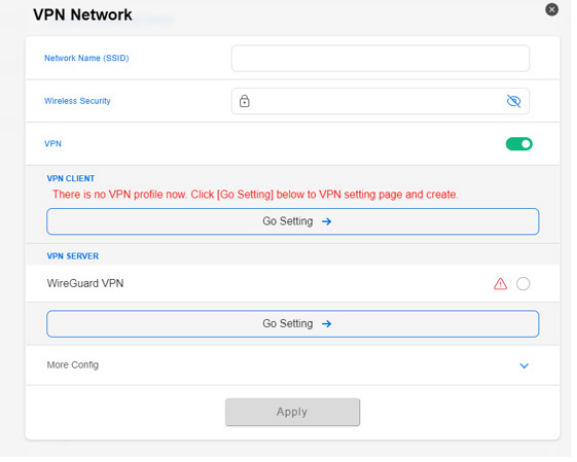
3.11.5 IoT Network

Allows you to set up a separate network for IoT devices easily. Recommended for use with surveillance devices, voice assistants, lighting, doorbell cams, smart locks and sensors.



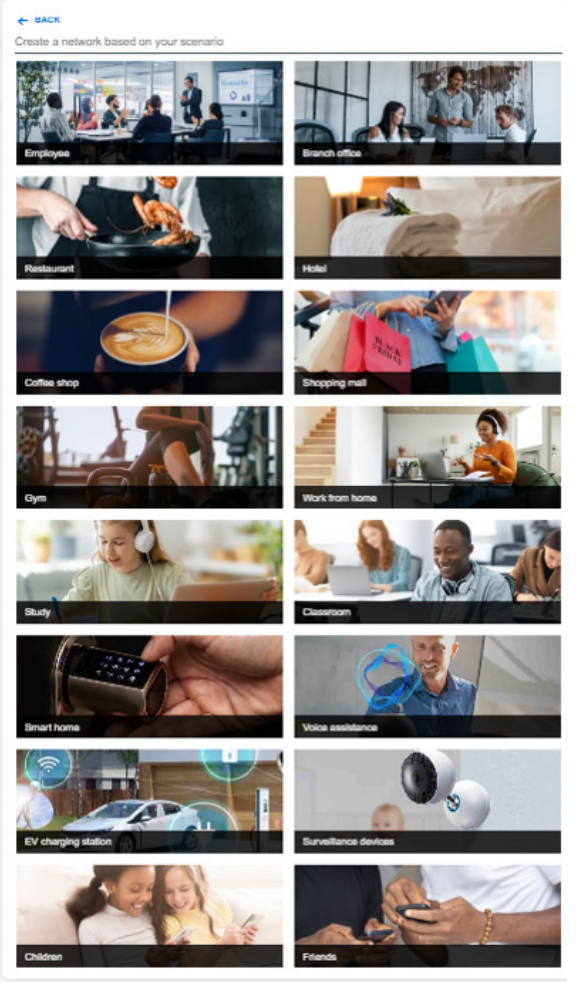
3.11.6 VPN Network

Helps establish a secure Internet connection using VPN.



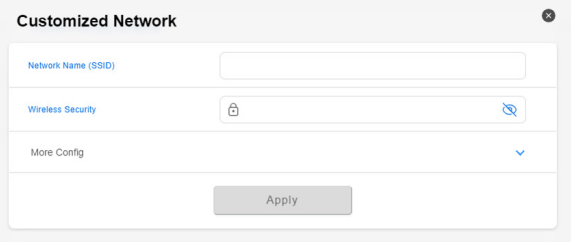
3.11.7 Scenario Explorer

If you have no idea which network to create, you can choose the sector that corresponds to your affiliation to create the network.



3.11.8 Customized Network

Allows you to select the option of a personalized network.



3.12 System Log

System Log contains your recorded network activities.

NOTE: System log resets when the router is rebooted or powered off.

To view your system log:

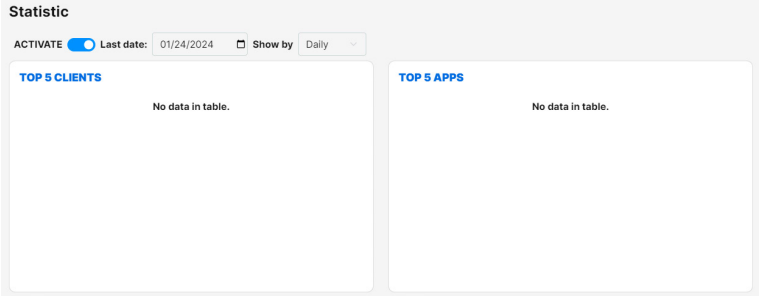
1. From the navigation panel, go to **Settings** > **System Log**.
2. You can view your network activities in any of these tabs:
   - General Log
   - DHCP Leases
   - Port Forwarding
   - Routing Table
   - IPv6
   - Connections

3.13 Traffic Analyzer

3.13.1 Traffic Analyzer

To use traffic analyzer:

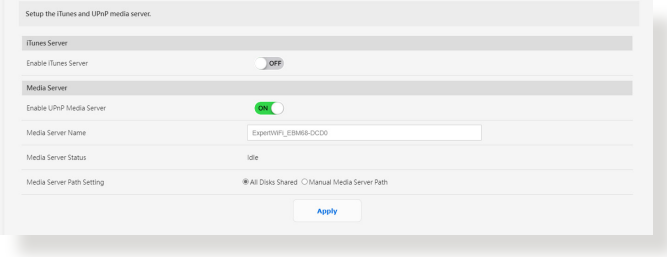
1. Turn on **ACTIVATE**.
2. Assign the last date to show, and choose to monitor network traffic on a daily, weekly or monthly basis from the **Show by** dropdown list.
3. The top five clients, top five apps, devices, client status and apps analysis will be displayed.



3.14 USB Application

3.14.1 Media Server

Media server allows you to set up the iTunes and UPnP server.



To launch the Media Server setting page, go to **Settings** > **USB Application** > **Media Server**.

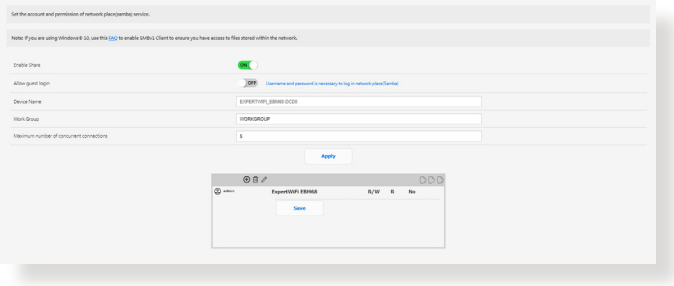
Refer to the following for the descriptions of the fields:

- **Enable iTunes Server**: Select ON/OFF to enable/disable the iTunes Server.
- **Enable UPnP Media Server** Select ON/OFF to enable/ disable the UPnP Media Server.
- **Media Server Name**: Enters the name of the media server.
- **Media Server Path Setting**: Select **All Disks Shared** or **Manual Media Server Path**.

When done, click **Apply**.

3.14.2 Network Place (Samba) Share

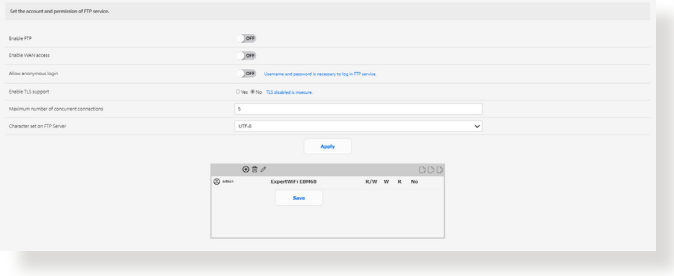
Network Place (Samba) Share allows you to set up the accounts and permissions for the Samba service.



To use Samba share, go to **Settings** > **USB Application** > **Network Place (Samba) Share**.

3.14.3 FTP Share

FTP Share allows you to set up the accounts and permissions for the FTP service.



To use FTP share, go to **Settings** > **USB Application** > **FTP Share**.

3.14.4 Network Printer Server

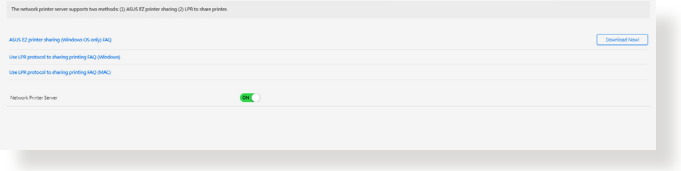
3.14.4.1 ASUS EZ Printer Sharing

ASUS EZ Printing Sharing utility allows you to connect a USB printer to your wired router's USB port and set up the print server. This allows your network clients to print and scan files wirelessly.

NOTE: The print server function is supported on Windows® 10 and Windows® 11.

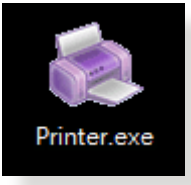
To set up the EZ Printer sharing mode:

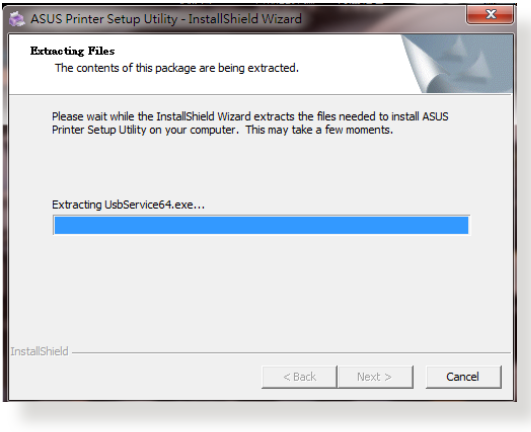
1. From the navigation panel, go to **Settings** > **USB Application** > **Network Printer Server**.
2. Click **Download Now!** to download the network printer utility.



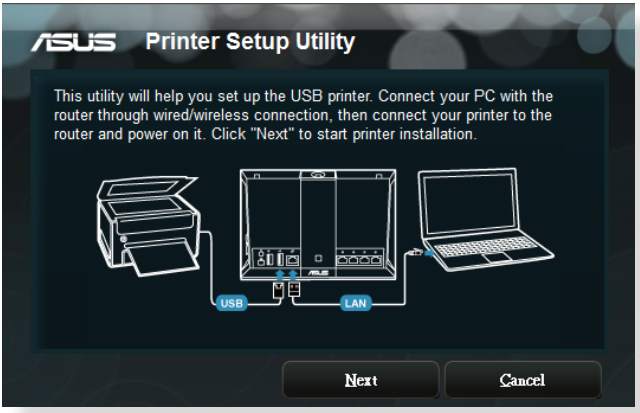
NOTE: Network printer utility is supported on Windows® 10 and Windows® 11 only. To install the utility on Mac OS, select **Use LPR protocol for sharing printer**.

3. Unzip the downloaded file and click the Printer icon to run the network printer setup program.



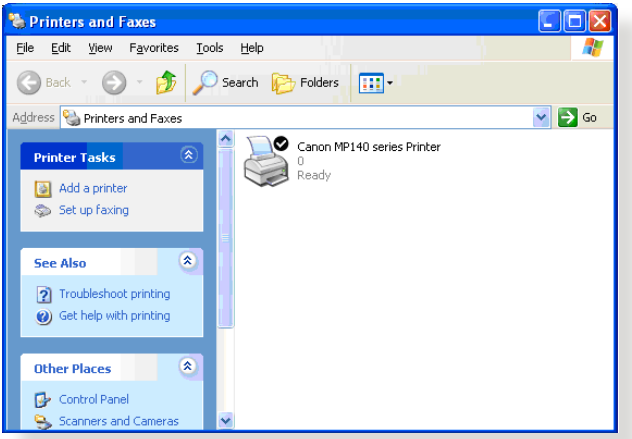


4. Follow the onscreen instructions to set up your hardware, then click **Next**.



5. Wait a few minutes for the initial setup to finish. Click **Next**.
6. Click **Finish** to complete the installation.
7. Follow the Windows® OS instructions to install the printer driver.

8. After the printer's driver installation is complete, network clients can now use the printer.

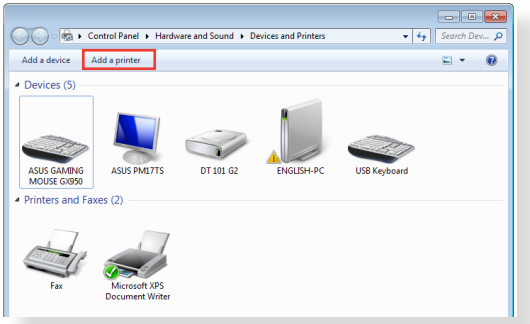


3.14.4.2 Using LPR to Share Printer

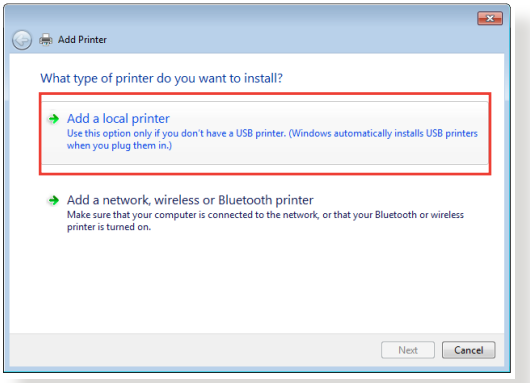
You can share your printer with computers running on Windows® and MAC operating system using LPR/LPD (Line Printer Remote/ Line Printer Daemon).

To share your LPR printer:

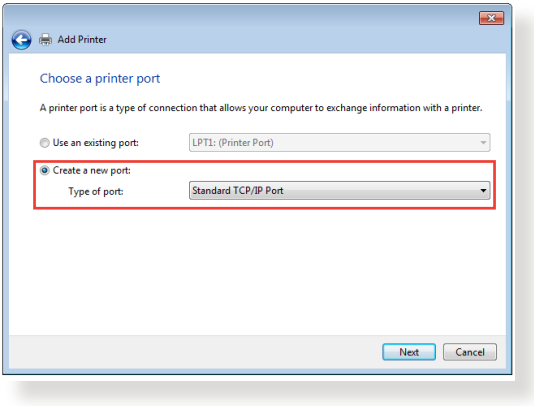
1. From the Windows® desktop, click **Start** > **Devices and Printers** > **Add a printer** to run the **Add Printer Wizard**.



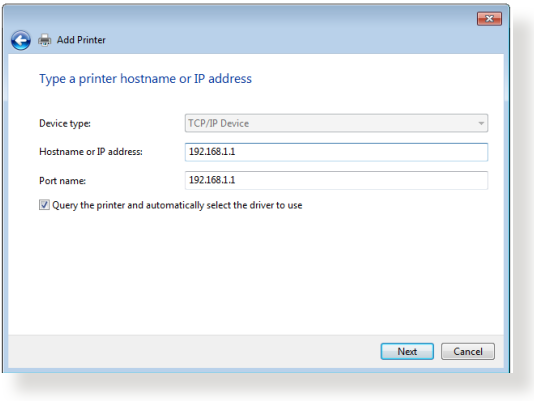
2. Select **Add a local printer** and then click **Next**.



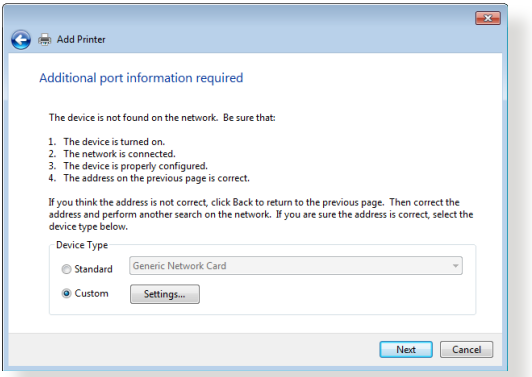
3. Select **Create a new port** then set **Type of Port** to **Standard TCP/IP Port**. Click **New Port**.



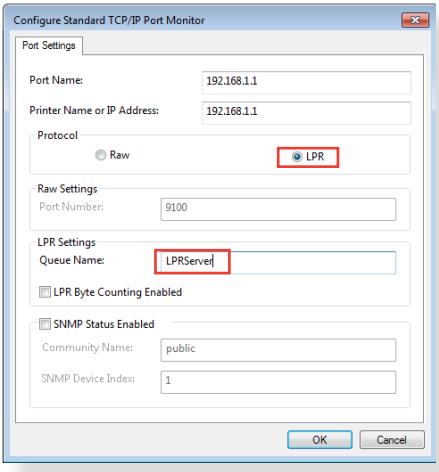
4. In the **Hostname or IP address** field, key in the IP address of the wired router then click **Next**.



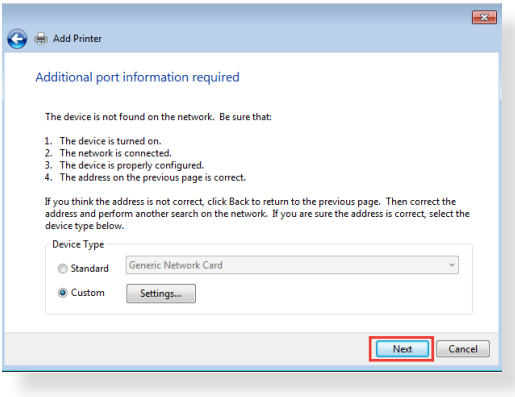
5. Select **Custom** then click **Settings**.



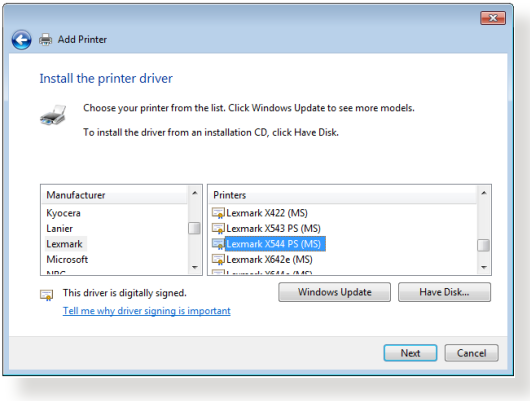
6. Set **Protocol** to **LPR**. In the **Queue Name** field, key in **LPRServer** then click **OK** to continue.



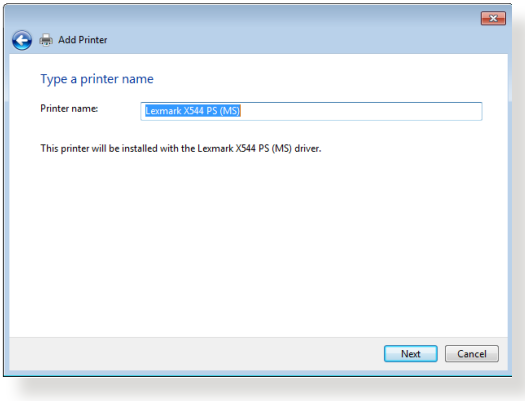
7. Click **Next** to finish setting up the standard TCP/IP port.



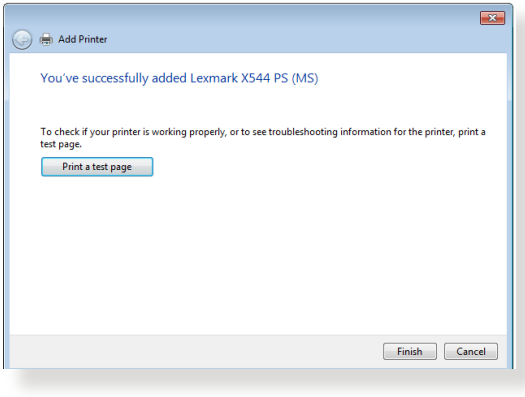
8. Install the printer driver from the vendor-model list. If your printer is not in the list, click **Have Disk** to manually install the printer drivers from a CD-ROM or file.



9. Click **Next** to accept the default name for the printer.



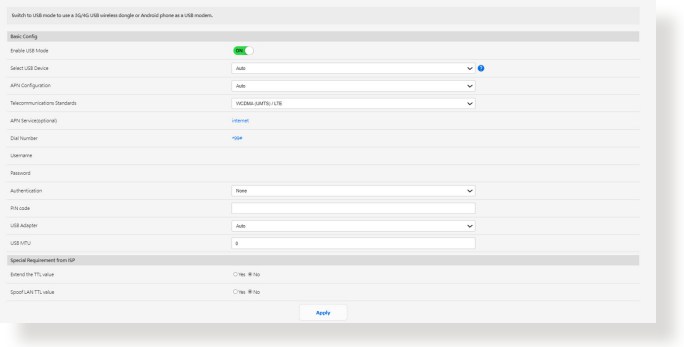
10. Click **Finish** to complete the installation.



3.14.5 USB Modem

Switch to the USB mode to use a 3G/4G USB wireless dongle or Android phone as a USB modem.

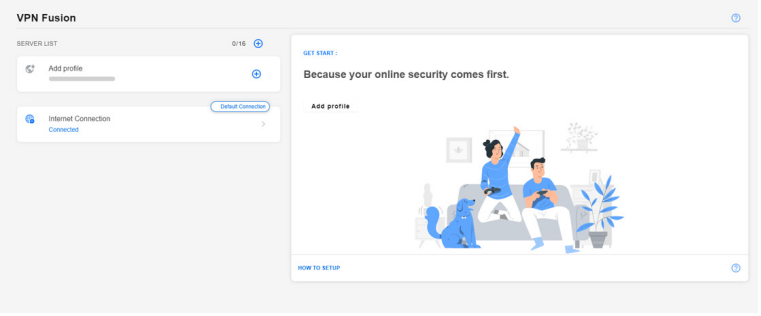
To use USB modem, go to **Settings** > **USB Application** > **USB Modem**.



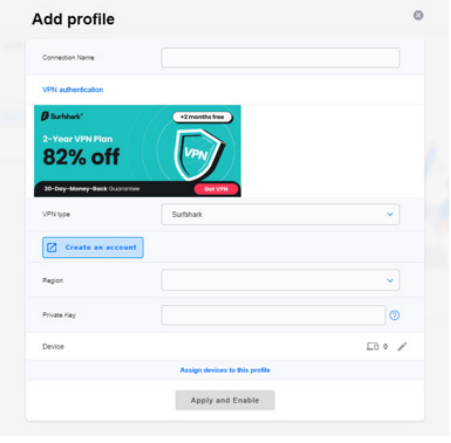
3.15 VPN Fusion

3.15.1 Creating a VPN fusion

VPN Fusion allows you to connect to multiple VPN servers simultaneously and assign your client devices to connect to different VPN tunnels.

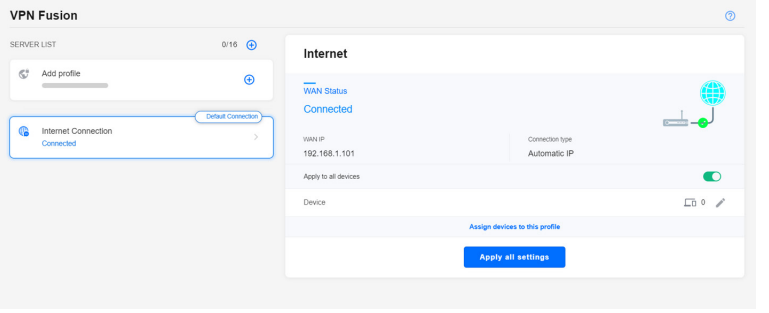


1. From the navigation panel, go to **VPN Fusion**.
2. Click ⊕ on the **Add profile** field to set up a new VPN tunnel.
3. Complete the VPN configuration including the connection name, VPN type, region, private key and device.
4. Click **Apply and Enable**.



3.15.2 Internet Connection

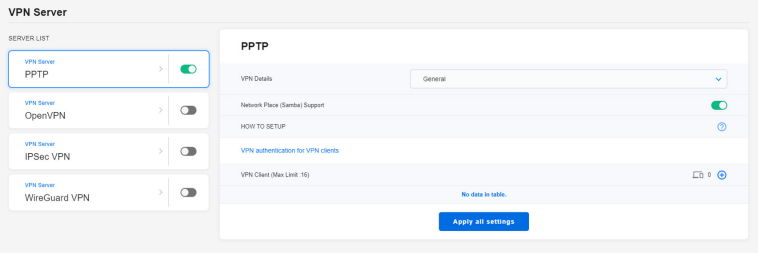
Allows you to manage the WAN status of the connected devices.



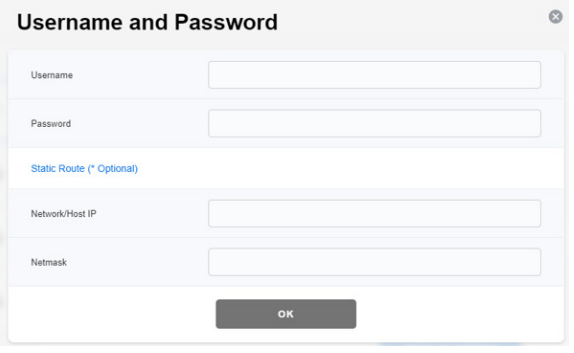
3.16 VPN Server

3.16.1 PPTP

1. From the navigation panel, go to **VPN Server** > **PPTP** and move the slider to the right (it is set to off on the left side by default).
2. On the **VPN Client (Max Limit: 16)** field, click ⊕ to add an account.



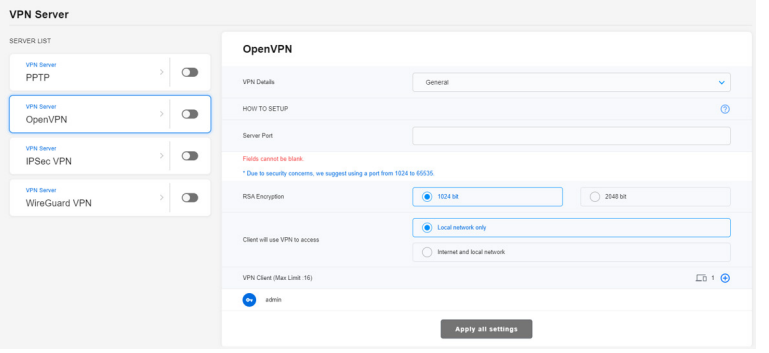
3. Enter customized *[Username]* and *[Password]*, and click **OK**.



NOTE: Once the *[Username]* and *[Password]* are set, they cannot be changed. For more information, please visit https://www.asus.com/support/FAQ/114892/.

3.16.2 OpenVPN

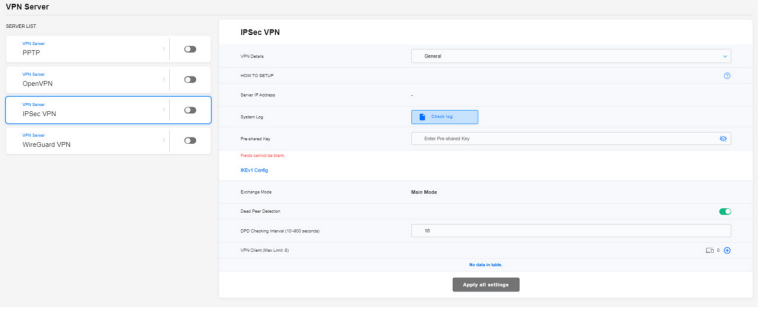
1. From the navigation panel, go to **VPN Server** > **OpenVPN** and move the slider to the right (it is set to off on the left side by default).
2. Configure the general settings in the **VPN Details** field.
3. Enter your username and password in the blank column.
4. On the **VPN Client (Max Limit: 16)** field, click ⊕ to add an account.
5. The password is automatically hidden. Click **Apply all settings**.



NOTE: For more information, please visit https://www.asus.com/support/FAQ/1008713/.

3.16.3 IPSec VPN

1. From the navigation panel, go to **VPN Server** > **IPSec VPN** and move the slider to the right (it is set to off on the left side by default).
2. Enter a key in the **Pre-sahred Key** field.
3. On the **VPN Client (Max Limit: 8)** field, click ⊕ to add an account.
5. Enter customized *[Username]* and *[Password]*, and click **Apply all settings**.

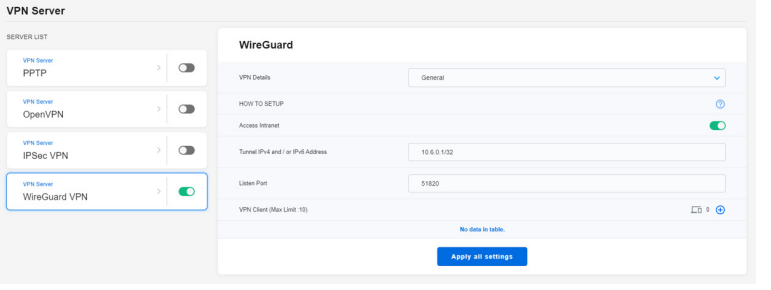


NOTE: Once the *[Username]* and *[Password]* are set, they cannot be changed. For more information, please visit https://www.asus.com/support/FAQ/1044190/.

3.16.4 WireGuard® VPN

1. From the navigation panel, go to **VPN Server** > **WireGuard VPN**.
2. On the **VPN Client (Max Limit: 10)** field, click ⊕ to add an account. For general devices such as laptops or smart phones, click **Apply**.
3. Click **Apply all settings** to enable the WireGuard® VPN.
4. Click " ••• " for more details.

NOTE: If you are using a smart phone to connect to WireGuard® VPN, please download WireGuard® app from Google Play or App Store, and scan the code in the app to download the configuration file.

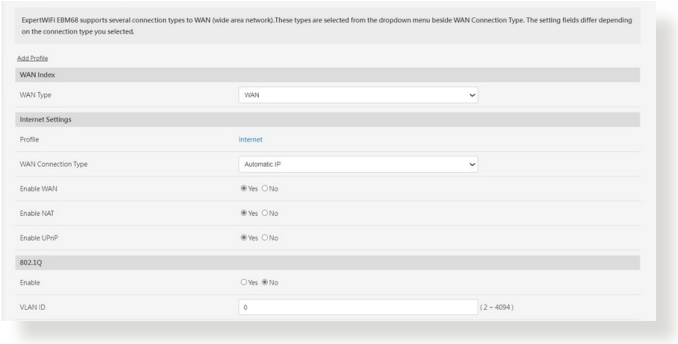


NOTE: For more information, please visit https://www.asus.com/support/FAQ/1048280/.

3.17 WAN

3.17.1 Internet Connection

The Internet Connection screen allows you to configure the settings of various WAN connection types.



To configure the WAN connection settings:

1. From the navigation panel, go to **Settings** > **WAN** > **Internet Connection**.
2. Configure the following settings below. When done, click **Apply**.

- **WAN Connection Type**: Choose your Internet Service Provider type. The choices are **Automatic IP**, **PPPoE**, **PPTP**, **L2TP** or **static IP**. Consult your ISP if the router is unable to obtain a valid IP address or if you are unsure the WAN connection type.
- **Enable WAN**: Select **Yes** to allow the router Internet access. Select **No** to disable Internet access.
- **Enable NAT**: NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.

- **Enable UPnP**: UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phone), to be controlled via an IP-based network with or without a central control through a gateway. UPnP connects PCs of all form factors, providing a seamless network for remote configuration and data transfer. Using UPnP, a new network device is discovered automatically. Once connected to the network, devices can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, which involves manually configuring port settings, UPnP automatically configures the router to accept incoming connections and direct requests to a specific PC on the local network.
- **Connect to DNS Server**: Allows this router to get the DNS IP address from the ISP automatically. A DNS is a host on the Internet that translates Internet names to numeric IP addresses.
- **Authentication**: This item may be specified by some ISPs. Check with your ISP and fill them in if required.
- **Host Name**: This field allows you to provide a host name for your router. It is usually a special requirement from your ISP. If your ISP assigned a host name to your computer, enter the host name here.
- **MAC Address**: MAC (Media Access Control) address is a unique identifier for your networking device. Some ISPs monitor the MAC address of networking devices that connect to their service and reject any unrecognized device that attempt to connect. To avoid connection issues due to an unregistered MAC address, you can:
  - Contact your ISP and update the MAC address associated with your ISP service.
  - Clone or change the MAC address of the ASUS wired router to match the MAC address of the previous networking device recognized by the ISP.

3.17.2 Multi-WAN

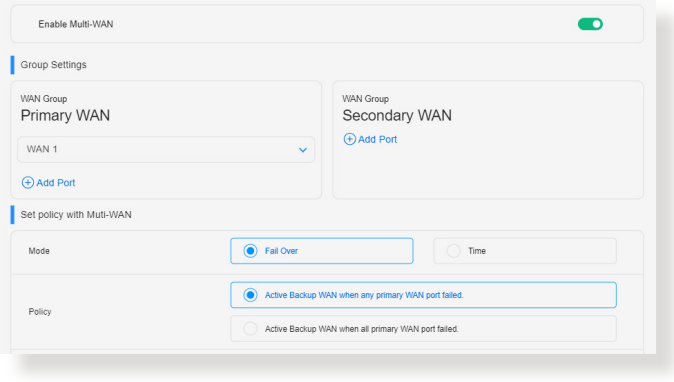
The Multi-WAN allows you to select multiple ISP connections to your router and the WAN groups for both primary and secondary WANs.

To configure Multi-WAN:

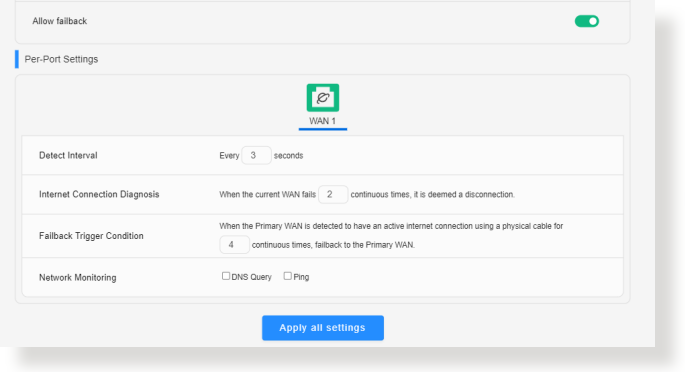
1. From the navigation panel, go to **Settings > WAN > Multi-WAN**.
2. Turn on **Enable Multi-WAN**.
3. Choose your **Primary WAN** and **Secondary WAN**. There are WAN, USB and Ethernet LAN for your options.
4. Choose **Fail Over** or **Time**.

   Fail Over: Use a secondary WAN for backup network access.

   Time: Set the time to schedule your Multi-WAN policy.
5. Choose **Active Backup WAN when any primary WAN port failed** or **Active Backup WAN when all primary WAN port failed**.



6. Turn on or off **Allow failback**.
7. Specify the detection interval.
8. Specify the number of continuous failure times before the current WAN is considered disconnected.
9. Specify the number of continuous times that the Primary WAN is detected as having an active internet connection via a physical cable, which triggers a failback to the Primary WAN.
10. Choose **DNS Query** or **Ping**.
11. Click **Apply all settings**.



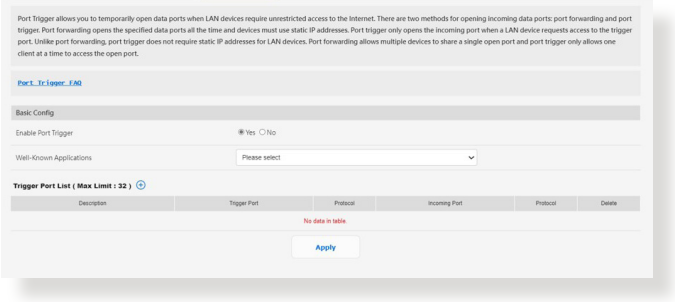
NOTE: Detailed explanations are available on the ASUS Support Site FAQ **https://www.asus.com/support/FAQ/1011719**.

3.17.3 Port Trigger

Port Trigger allows you to temporarily enable data ports when LAN devices require unrestricted access to the Internet. There are two methods for opening incoming data ports: port forwarding and port trigger.

- Port forwarding enables the specified data ports all the time and devices must use static IP addresses.
- Port trigger only enables the incoming port when a LAN device requests access to the trigger port.

Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows multiple devices to share a single open port and port trigger only allows one client at a time to access the open port.



To set up Port Trigger:

1. From the navigation panel, go to **Settings** > **WAN** > **Port Trigger**.
2. Configure the following settings below. When done, click **Apply**.
   - **Enable Port Trigger**: Choose **Yes** to enable Port Trigger.
   - **Well-Known Applications**: Select popular games and web services to add to the Port Trigger List.
   - **Description**: Enter a short name or description for the service.

- **Trigger Port**: Specify a trigger port to open the incoming port.
- **Protocol**: Select the protocol, TCP, or UDP.
- **Incoming Port**: Specify an incoming port to receive inbound data from the Internet.

NOTES:

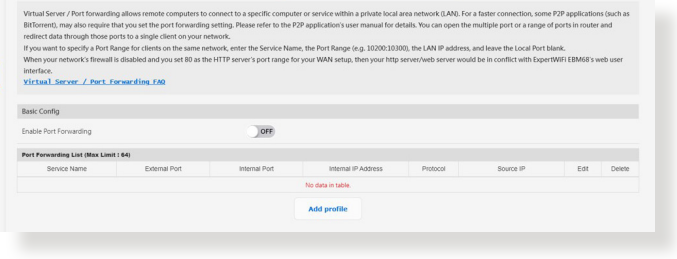
- When connecting to an IRC server, a client PC makes an outgoing connection using the trigger port range 66660-7000. The IRC server responds by verifying the username and creating a new connection to the client PC using an incoming port.
- If Port Trigger is disabled, the router drops the connection because it is unable to determine which PC is requesting for IRC access. When Port Trigger is enabled, the router assigns an incoming port to receive the inbound data. This incoming port closes once a specific time period has elapsed because the router is unsure when the application has been terminated.
- Port triggering only allows one client in the network to use a particular service and a specific incoming port at the same time.
- You cannot use the same application to trigger a port in more than one PC at the same time. The router will only forward the port back to the last computer to send the router a request/trigger.
- For more information, please visit https://www.asus.com/support/FAQ/114110.

3.17.4 Virtual Server/Port Forwarding

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a faster connection, some P2P applications (such as BitTorrent) may also require that you set the port forwarding setting. Please refer to the P2P application's user manual for details. You can enable multiple ports or a range of ports in the router and redirect data through those ports to a single client on your network.

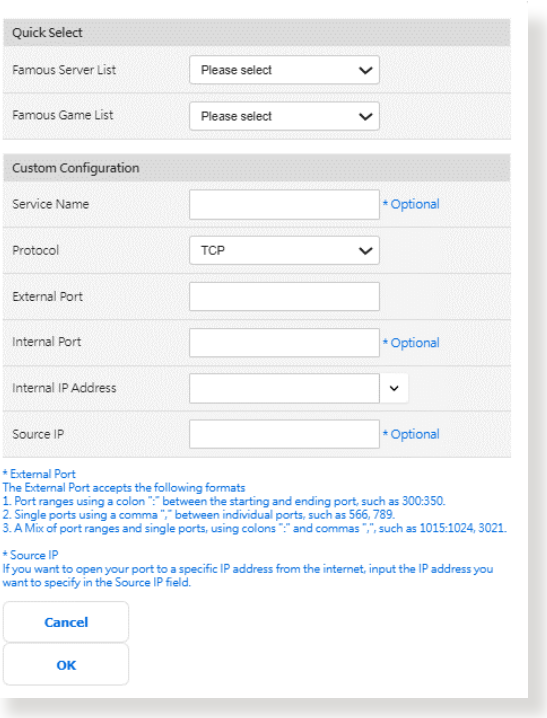
If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200:10300), the LAN IP address, and leave the Local Port blank.

NOTE: When port forwarding is enabled, the ASUS router blocks unsolicited inbound traffic from the Internet and only allows replies from outbound requests from the LAN. The network client does not have access to the Internet directly, and vice versa.



To set up Port Forwarding:

1. From the navigation panel, go to **Settings** > **WAN** > **Virtual Server / Port Forwarding**.
2. Slide the bar to **ON** to enable Port Forwarding, then click **Add Profile**. After configuring the following settings, click **OK**.



- **Famous Server List**: Determine which type of service you want to access.
- **Famous Game List**: This item lists ports required for popular online games to work correctly.
- **Service Name**: Enter a service name.
- **Protocol**: Select the protocol. If you are unsure, select **BOTH**.
- **External Port**: Accept the following formats:
  1) A port range using a colon ":" in the middle to specify the upper and lower limits of the range, such as 300:350;
  2) Individual port numbers using a comma "," to separate them, such as 566, 789;
  3) A Mix of port ranges and individual ports, using colons ":" and commas ",", such as 1015:1024, 3021.

- **Internal Port**: Enter a specific port to receive forwarded packets. Leave this field blank if you want the incoming packets to be redirected to the specified port range.
- **Internal IP Address**: Key in the client's LAN IP address.
- **Source IP**: If you want to open your port to a specific IP address from the Internet, input the IP address you want to give access to in this field.

NOTE: Use a static IP address for the local client to make port forwarding work properly. Refer to section **3.9 LAN** for information.

To check if Port Forwarding has been configured successfully:

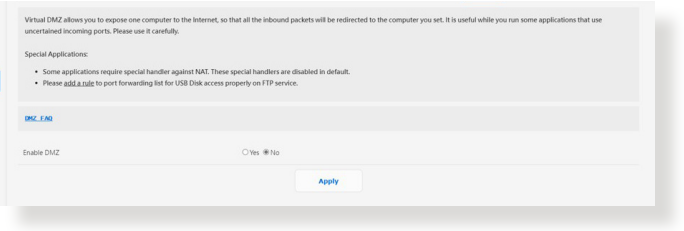
- Ensure that your server or application is set up and running.
- You will need a client outside your LAN but has Internet access (referred to as "Internet client"). This client should not be connected to the ASUS router.
- On the Internet client, use the router's WAN IP to access the server. If port forwarding has been successful, you should be able to access the files or applications.

Differences between port trigger and port forwarding:

- Port triggering will work even without setting up a specific LAN IP address. Unlike port forwarding, which requires a static LAN IP address, port triggering allows dynamic port forwarding using the router. Predetermined port ranges are configured to accept incoming connections for a limited period of time. Port triggering allows multiple computers to run applications that would normally require manually forwarding the same ports to each PC on the network.
- Port triggering is more secure than port forwarding since the incoming ports are not open all the time. They are opened only when an application is making an outgoing connection through the trigger port.

3.17.5 DMZ

Virtual DMZ allows you to expose one computer to the Internet, so that all the inbound packets will be redirected to the computer you set. It is useful while you run some applications that use uncertain incoming ports. Please use it with care.



To set up DMZ:

1. From the navigation panel, go to **Settings** > **WAN** > **DMZ**.
2. Configure the setting below. When done, click **Apply**.
   - **IP address of Exposed Station:** Key in the client's LAN IP address that will provide the DMZ service and be exposed on the Internet. Ensure that the server client has a static IP address.

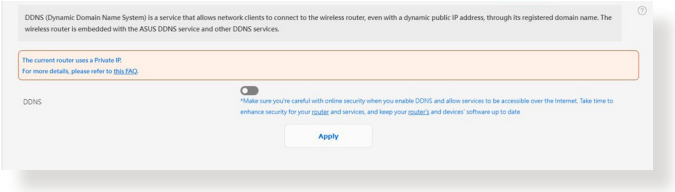
To remove DMZ:

1. Delete the client's LAN IP address from the **IP Address of Exposed Station** text box.
2. When done, click **Apply**.

NOTE: For more information, please visit https://www.asus.com/support/FAQ/1011723.

3.17.6 DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wired router, even with a dynamic public IP address, through its registered domain name. The wired router is embedded with the ASUS DDNS service and other DDNS services.



To set up DDNS:

1. From the navigation panel, go to **Settings** > **WAN** > **DDNS**.
2. Configure the following settings below. When done, click **Apply**.
   - **Enable the DDNS Client**: Enable DDNS to access the ASUS router via the DNS name rather than WAN IP address.
   - **Server and Host Name**: Choose ASUS DDNS or other DDNS. If you want to use ASUS DDNS, fill in the Host Name in the format of xxx.asuscomm.com (xxx is your host name).
   - If you want to use a different DDNS service, click FREE TRIAL and register online first. Fill in the User Name or E-mail Address and Password or DDNS Key fields.
   - **Enable wildcard**: Enable wildcard if your DDNS service requires one.

NOTES:

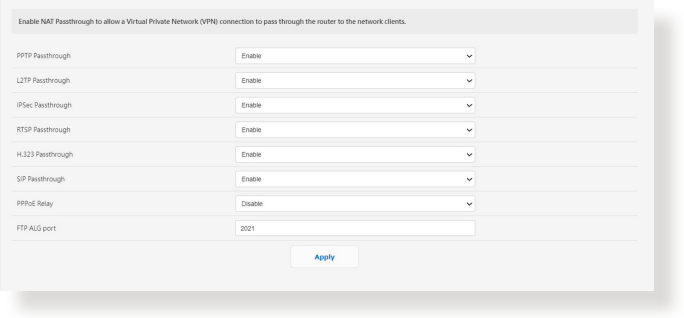
DDNS service will not work under these conditions:

- When the wired router is using a private WAN IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x), as indicated by a yellow text.
- The router may be on a network that uses multiple NAT tables.

3.17.7 NAT Passthrough

Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.

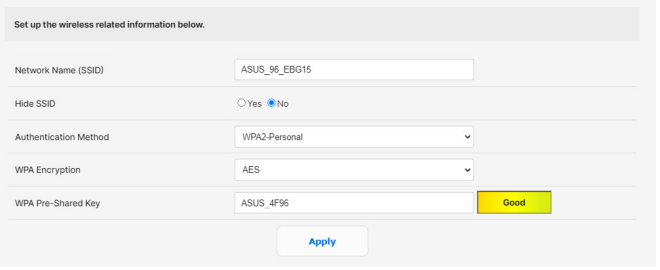
To set up NAT Passthrough, go to **Settings** > **WAN** > **NAT Passthrough**. When done, click **Apply**.



3.18 Wireless

3.18.1 General

The **General** tab allows you to configure the basic wireless settings.



To configure the basic wireless settings:

1. From the navigation panel, go to **Settings** > **Wireless** > **General**.
2. Assign a unique name for your SSID (Service Set Identifier) or network name to identify your wireless network. Wi-Fi devices can identify and connect to the wireless network via your assigned SSID. The SSIDs on the information banner are updated once new SSIDs are saved to the settings.

IMPORTANT! To make the Wi-Fi function available, ensure to integrate a wireless Access Point (AP) such as ExpertWiFi EBA63 or router such as ExpertWiFi EBR63 or ExpertWiFi EBM68 into the EBG15's AiMesh network.

---

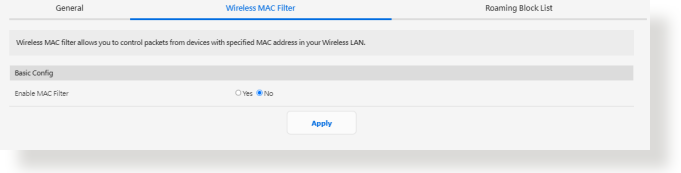
3. In the **Hide SSID** field, select **Yes** to prevent wireless devices from detecting your SSID. When this function is enabled, you would need to enter the SSID manually on the wireless device to access the wireless network.
4. Select any of these authentication methods:
   - **Open System**: This option provides no security.

- **WPA/WPA2/WPA3-Personal**: This option provides strong security. You can use either WPA (with TKIP) or WPA2 (with AES). If you select this option, you must use TKIP + AES encryption and enter the WPA passphrase (network key).
- **WPA/WPA2/WPA3-Enterprise**: This option provides very strong security. It is with integrated EAP server or an external RADIUS back-end authentication server.

5. Assign a unique password for your WPA pre-shared key.

3.18.2 Wireless MAC Filter

Wireless MAC filter provides control over packets transmitted to a specified MAC (Media Access Control) address on your wireless network.

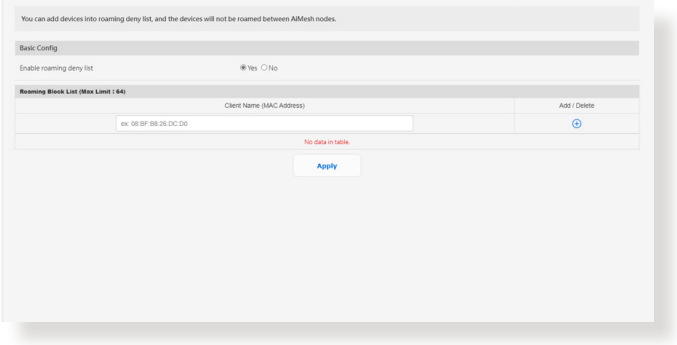


To set up the Wireless MAC filter:

1. From the navigation panel, go to **Settings** > **Wireless** > **Wireless MAC Filter**.
2. Tick **Yes** in the **Enable Mac Filter** field.
3. In the **MAC Filter Mode** dropdown list, select either **Accept** or **Reject**.
   - Select **Accept** to allow devices in the MAC filter list to access to the wireless network.
   - Select **Reject** to prevent devices in the MAC filter list to access to the wireless network.
4. On the MAC filter list, click ⊕ and key in the MAC address of the wireless device.
5. Click **Apply**.

3.18.3 Roaming Block List

The feature allows you to add devices to the roaming block list and prevent them from roaming between AiMesh nodes.



4 Troubleshooting

This chapter provides solutions for issues you may encounter with your router. If you encounter problems that are not mentioned in this chapter, visit the ASUS support site at: https://www.asus.com/support/ for more product information and contact details of ASUS Technical Support.

4.1 Basic Troubleshooting

If you are having problems with your router, try these basic steps in this section before looking for further solutions.

Upgrade Firmware to the latest version.

1. From the navigation panel, go to **Settings** > **Administration** > **Firmware Upgrade**. Click **Check** to verify if the latest firmware is available.
2. If the latest firmware is available, visit the ASUS global website to download the latest firmware.
3. From the **Firmware Upgrade** page, click **Browse** to upload the firmware file.
4. Click **Upload** to upgrade the firmware.

Restart your network in the following sequence:

1. Turn off the modem.
2. Unplug the modem.
3. Turn off the router and computers.
4. Plug in the modem.
5. Turn on the modem and then wait for 2 minutes.
6. Turn on the router and then wait for 2 minutes.
7. Turn on computers.

Check if your Ethernet cables are plugged properly.

- When the Ethernet cable connecting the router with the modem is plugged in properly, the WAN LED will be on.
- When the Ethernet cable connecting your powered-on computer with the router is plugged in properly, the corresponding LAN LED will be on.

Check if your network settings are correct.

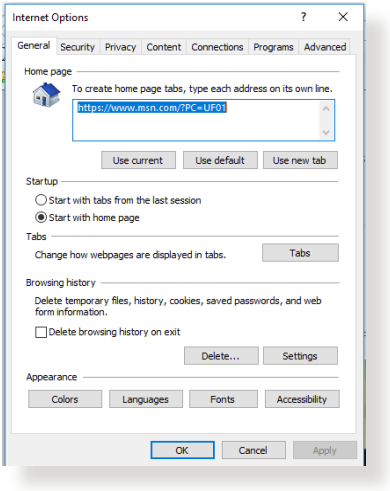
- Each client on the network should have a valid IP address. ASUS recommends that you use the wired router's DHCP server to assign IP addresses to computers on your network.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the web GUI, **Dashboard** > **Clients**.

4.2 Frequently Asked Questions (FAQs)

I cannot access the router GUI using a web browser

- If your computer is wired, check the Ethernet cable connection and LED status as described in the previous section.
- Ensure that you are using the correct login information. Ensure that the Caps Lock key is disabled when you enter the login information.
- Delete the cookies and files in your web browser. For Internet Explorer, follow these steps:

  1. Launch Internet Explorer, then click **Tools** > **Internet Options**.
  2. In the **General** tab, under **Browsing history**, click **Delete…**, select **Temporary Internet files and website files** and **Cookies and website data** then click **Delete**.



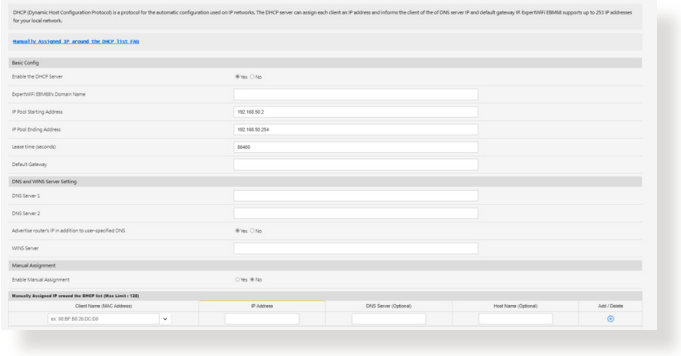
NOTES:

- The commands for deleting cookies and files vary with web browsers.
- Disable proxy server settings, cancel the dial-up connection, and set the TCP/IP settings to obtain IP addresses automatically. For more details, refer to Chapter 1 of this user manual.
- Ensure that you use CAT5e or CAT6 ethernet cables.

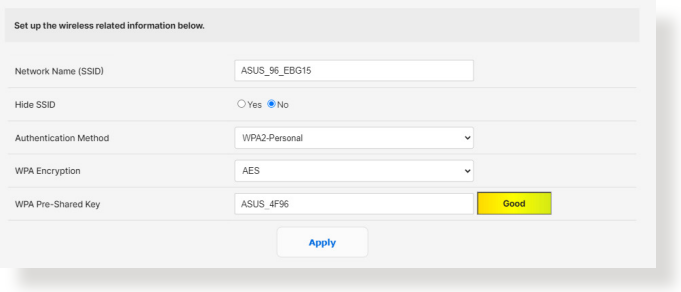
The client cannot establish a wireless connection with the router.

IMPORTANT! To make the Wi-Fi function available, ensure to integrate a wireless Access Point (AP) such as ExpertWiFi EBA63 or router such as ExpertWiFi EBR63 or ExpertWiFi EBM68 into the EBG15's AiMesh network.

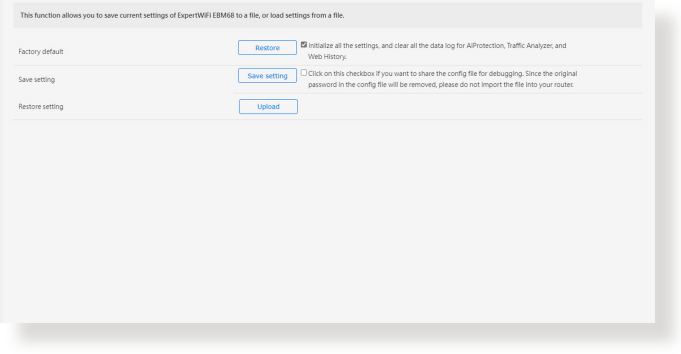
- **DHCP server has been disabled:**
  1. Launch the web GUI. Go to **Dashboard** > **Clients** and search for the device that you want to connect to the router.
  2. If you cannot find the device in the **Dashboard**, go to **Settings** > **LAN** > **DHCP Server**.



- SSID has been hidden. If your device can find SSIDs from other routers but cannot find your router's SSID, go to **Settings** > **Wireless** > **General**, select **NO** on **Hide SSID**.



- If you are using a wireless LAN adapter, check if the wireless channel in use conforms to the channels available in your country/area. If not, adjust the channel, channel bandwidth, and wireless mode.
- If you still cannot connect to the router wiredly, you can reset your router to factory default settings. In the router GUI, click **Settings** > **Administration** > **Restore/Save/Upload Setting** and click **Restore**.



Internet is not accessible.

- Check if your router can connect to your ISP's WAN IP address. To do this, launch the web GUI and go to **Dashboard**, and check the Internet status.
- If your router cannot connect to your ISP's WAN IP address, try restarting your network as described in the section **Restart your network in following sequence** under **Basic Troubleshooting**.
- If there is still no Internet access, try to reboot your computer and verify the network's IP address and gateway address.
- Check the status indicators on the ADSL modem and the wired router. If the WAN LED on the wired router is not ON, check if all cables are plugged properly.

You forgot the SSID (network name) or network password

- Setup a new SSID and encryption key via a wired connection (Ethernet cable). Launch the web GUI, go to **Dashboard**, click the router icon, enter a new SSID and encryption key, and then click **Apply**.
- Reset your router to the default settings. Launch the web GUI, go to **Settings** >**Administration** > **Restore/Save/Upload Setting**, and click **Restore**.

How to restore the system to its default settings?

- Go to **Settings** > **Administration** > **Restore/Save/Upload Setting**, and click **Restore**.

Firmware upgrade failed.

Launch the rescue mode and run the Firmware Restoration utility.

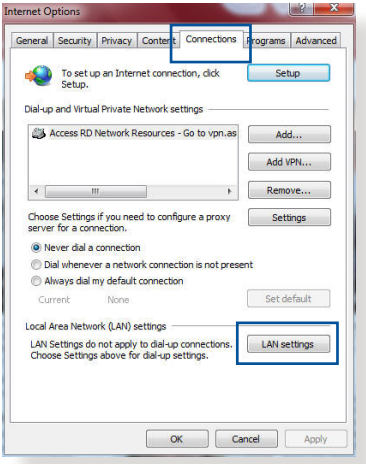
Cannot access Web GUI

Before configuring your wired router, do the steps described in this section for your host computer and network clients.

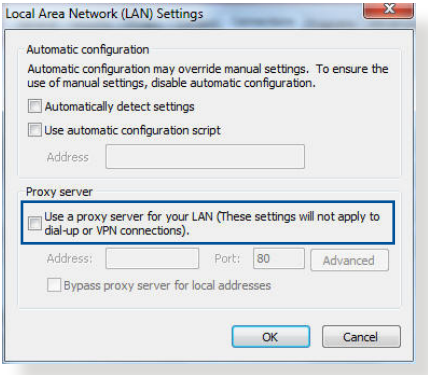
A. Disable the proxy server, if enabled.

Windows®

1. Click **Start > Internet Explorer** to launch the browser.
2. Click **Tools** > **Internet options** > **Connections** > **LAN settings**.

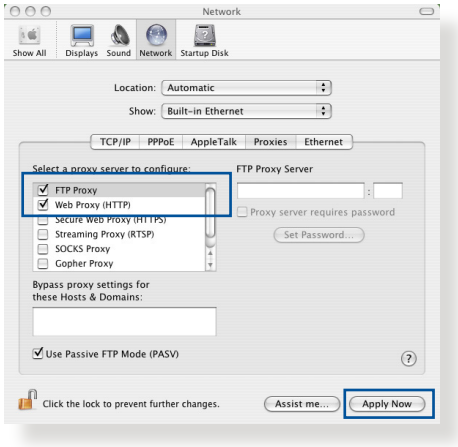


3. From the Local Area Network (LAN) Settings screen, untick **Use a proxy server for your LAN**.
4. Click **OK** when done.



MAC OS

1. From your Safari browser, click **Safari** > **Preferences** > **Advanced** > **Change Settings...**
2. From the Network screen, deselect **FTP Proxy** and **Web Proxy (HTTP)**.
3. Click **Apply Now** when done.

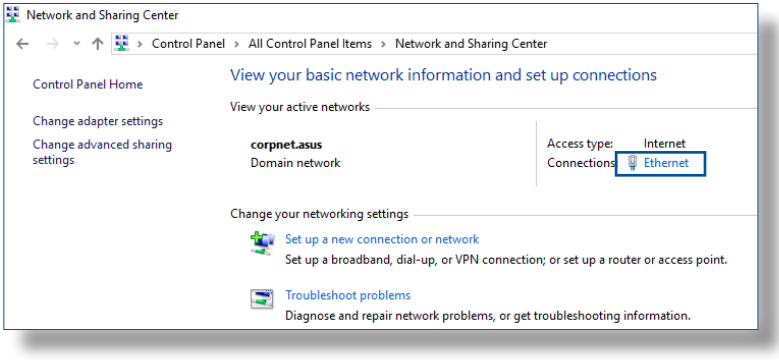


NOTE: Refer to your browser's help feature for details on disabling the proxy server.

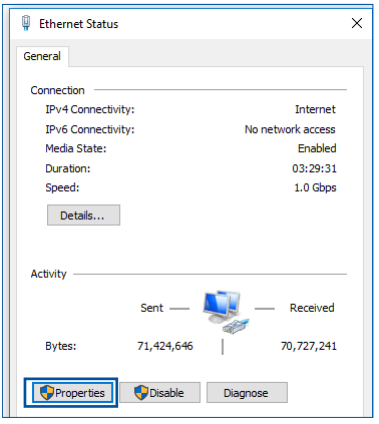
B. Set the TCP/IP settings to automatically obtain an IP address.

Windows®

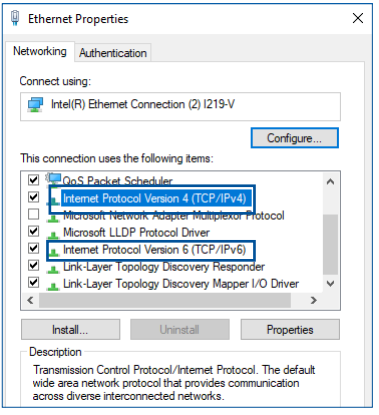
1. Click **Start** > **Control Panel** > **Network and Sharing Center,** then click the network connection to display its status window.



2. Click **Properties** to display the Ethernet Properties window.



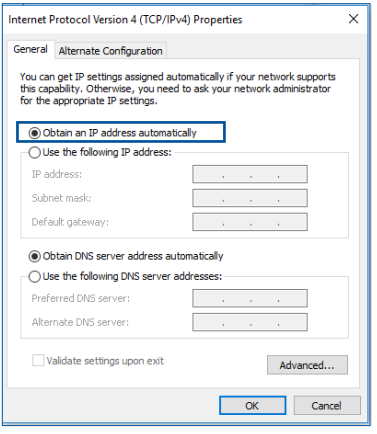
3. Select **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, then click **Properties**.



4. To obtain the IPv4 IP settings automatically, tick **Obtain an IP address automatically**.

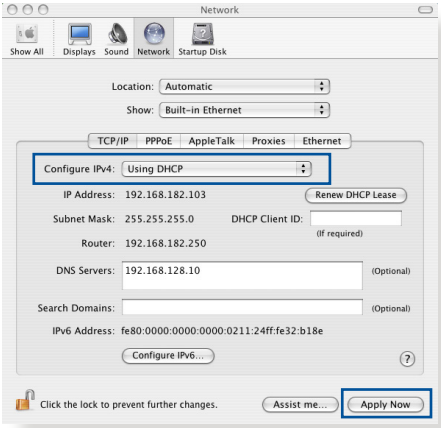
   To obtain the IPv6 IP settings automatically, tick **Obtain an IPv6 address automatically**.

5. Click **OK** when done.



MAC OS

1. Click the Apple icon located on the top left of your screen.
2. Click **System Preferences** > **Network** > **Configure...**
3. From the **TCP/IP** tab, select **Using DHCP** in the **Configure IPv4** dropdown list.
4. Click **Apply Now** when done.

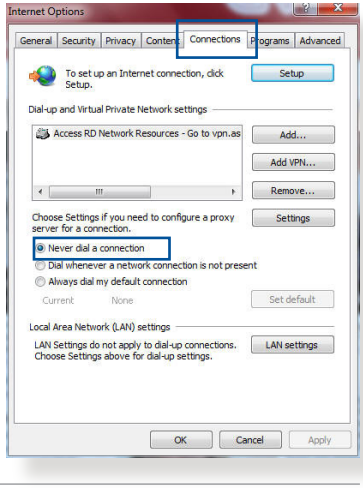


NOTE: Refer to your operating system's help and support feature for details on configuring your computer's TCP/IP settings.

C. Disable the dial-up connection, if enabled.

Windows®

1. Click **Start** > **Internet Explorer** to launch the browser.
2. Click **Tools** > **Internet options** > **Connections**.
3. Tick **Never dial a connection**.
4. Click **OK** when done.



NOTE: Refer to your browser's help feature for details on disabling the dial-up connection.

Appendices

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance

on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

    For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Safety Notices

When using this product, always follow the fundamental safety precautions, including, but not limited to the following:

WARNING!

- The power supply cord(s) must be plugged into socket-outlet(s) that is /are provided with a suitable earth ground. Connect the equipment only to a nearby socket outlet that is easily accessible.
- If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- DO NOT use damaged power cords, accessories, or other peripherals.
- DO NOT mount this equipment higher than 2 meters.
- Use this product in environments with ambient temperatures between 0°C (32°F) and 40°C (104°F).
- Read the operational guidelines and the temperature range provided before using the product.
- Pay particular attention to the personal safety when using this device in airports, hospitals, gas stations and professional garages.
- Medical device interference: Maintain a minimum distance of at least 15 cm (6 inches) between implanted medical devices and ASUS products to reduce the risk of interference.
- Kindly use ASUS products in good reception conditions to minimize the radiation's level.
- Keep the device away from pregnant women and the lower abdomen of the teenager.
- DO NOT use this product if visible defects can be observed or it has been wet or damaged or modified. Seek servicing for assistance.

WARNING!

- DO NOT place on uneven or unstable work surfaces.
- DO NOT place or drop objects on the top of the product. Avoid exposing the product to mechanical shock such as crushing, bending, puncturing or shredding.
- DO NOT disassemble, open, microwave, incinerate, paint, or shove any foreign objects into this product.
- Refer to the rating label on the bottom of your product and ensure your power adapter complies with this rating.
- Keep the product away from fire and heat sources.
- DO NOT expose to or use near liquids, rain, or moisture. DO NOT use the product during electrical storms.
- Connect the PoE output circuits of this product exclusively to PoE networks, without routing to external facilities.
- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- Only use accessories that have been approved by the device manufacturer to work with this model. The use of other types of accessories may invalidate the warranty or violate local regulations and laws, and may pose safety risks. Contact your local retailer for the availablity of authorized accessories.
- Use of this product in a way not recommended in the provided instructions may result in a risk of fire or personal injury.

Service and Support

Visit our multi-language website at https://www.asus.com/support.